aws

사용자 가이드

아마존 DataZone

아마존 DataZone: 사용자 가이드

Table of Contents

아마존이란 DataZone 무엇입니까?

DataZone Amazon은 온프레미스 및 타사 소스에 저장된 데이터를 더 빠르고 쉽게 카탈로그, 검색, 공유 및 관리할 수 있게 해주는 데이터 관리 서비스입니다. AWS DataZoneAmazon을 사용하면 조직의 데이터 자산을 감독하는 관리자가 세밀한 제어를 통해 데이터 액세스를 관리하고 제어할 수 있습니다. 이러한 제어를 통해 적절한 수준의 권한과 컨텍스트로 액세스를 보장할 수 있습니다. Amazon을 DataZone 사용하면 엔지니어, 데이터 과학자, 제품 관리자, 분석가 및 비즈니스 사용자가 조직 전체에서 데이터를 쉽게 공유하고 액세스하여 데이터를 발견하고 사용하고 협업하여 데이터 기반 통찰력을 도출할 수 있습니다.

DataZone Amazon은 Amazon Redshift, Amazon Athena, Amazon, QuickSight Glue AWS , Lake AWS Formation, 온프레미스 소스, 타사 소스 등을 비롯한 데이터 관리 서비스를 통합하여 최종 사용자에게 직접 데이터를 전달하고 아키텍처를 단순화할 수 있도록 지원합니다.

주제

Amazon으로 무엇을 할 수 있나요 DataZone?

DataZoneAmazon에서는 다음과 같은 작업을 수행할 수 있습니다.

- 조직 경계를 초월한 데이터 액세스를 관리합니다. DataZoneAmazon을 사용하면 개별 자격 증명을 사용하지 않고도 조직의 보안 규정에 따라 올바른 사용자가 올바른 목적으로 올바른 데이터에 액세스하도록 할 수 있습니다. 또한 통제된 워크플로를 통해 데이터 자산 사용에 투명성을 제공하고 데이터 구독을 승인할 수 있습니다. 또한 사용 감사 기능을 통해 프로젝트 전반의 데이터 자산을 모니터링할 수 있습니다.
- 공유 데이터 및 도구를 통해 데이터 작업자를 연결하여 비즈니스 통찰력을 확보하세요. DataZoneAmazon을 사용하면 팀 간에 원활하게 협업하고 데이터 및 분석 도구에 대한 셀프 서비스 액세스를 제공하여 비즈니스 팀의 효율성을 높일 수 있습니다. 비즈니스 용어를 사용하여 온프레미스 또는 타사 공급자와 함께 저장된 카탈로그 데이터를 검색 AWS, 공유 및 액세스할 수 있습니다. 또한 Amazon DataZone 비즈니스 용어집을 사용하여 사용하려는 데이터에 대해 자세히 알아볼 수 있습니다.

- 기계 학습으로 데이터 검색 및 카탈로그 작성을 자동화하십시오. DataZoneAmazon을 사용하면 비즈니스 데이터 카탈로그에 데이터 속성을 수동으로 입력하는 데 소요되는 시간을 줄일 수 있습니다. 데이터 카탈로그의 데이터가 풍부해지면 검색 환경도 개선됩니다.

DataZone Amazon은 어떻게 다른 AWS 서비스를 지원하고 통합합니까?

DataZone Amazon은 다른 AWS 서비스와의 세 가지 유형의 통합을 지원합니다.

- 생산자 데이터 소스 - AWS Glue 데이터 DataZone 카탈로그 및 Amazon Redshift 테이블 및 뷰에 저장된 데이터에서 Amazon 카탈로그에 데이터 자산을 게시할 수 있습니다. Amazon Simple Storage Service (S3) 의 객체를 Amazon 카탈로그에 수동으로 게시할 수도 있습니다. DataZone
- 소비자 도구 - Amazon Athena 또는 Amazon Redshift 쿼리 편집기를 사용하여 데이터 자산에 액세스하고 분석할 수 있습니다.
- 액세스 제어 및 주문 처리 - 아마존은 AWS Lake Formation에서 관리하는 AWS Glue 테이블과 Amazon Redshift 테이블 및 뷰에 대한 액세스 권한 부여를 DataZone 지원합니다. 기타 모든 데이터 자산의 경우 Amazon은 사용자의 활동 (예: 구독 요청에 대한 승인) 과 관련된 표준 이벤트를 EventBridge Amazon에 DataZone 게시합니다. 이러한 표준 이벤트를 사용하여 사용자 지정 통합을 위해 다른 AWS 서비스 또는 타사 솔루션과 통합할 수 있습니다.

Amazon에 액세스하려면 어떻게 해야 DataZone 합니까?

다음 방법 중 하나로 DataZone Amazon에 액세스할 수 있습니다.

- 아마존 DataZone 콘솔

  Amazon DataZone 관리 콘솔을 사용하여 Amazon DataZone 도메인, 블루프린트 및 사용자에 액세스하고 구성할 수 있습니다. 자세한 내용은 https://console.aws.amazon.com/datazone 을 참조하십시오. Amazon DataZone 관리 콘솔은 Amazon DataZone 데이터 포털을 생성하는 데도 사용됩니다.
- 아마존 DataZone 데이터 포털

  Amazon DataZone 데이터 포털은 셀프 서비스 방식으로 데이터를 카탈로그, 검색, 관리, 공유 및 분석할 수 있는 브라우저 기반 웹 애플리케이션입니다. 데이터 포털은 IAM Identity Center (AWS SSO 의 후속) 를 통해 ID 공급자가 제공하는 자격 증명 또는 AWS IAM 자격 증명으로 사용자를 인증할 수 있습니다. Amazon DataZone 콘솔 https://console.aws.amazon.com/datazone 에 액세스하여 데이터 포털 URL을 확인할 수 있습니다.

- 아마존 DataZone HTTPS API

  서비스에 직접 HTTPS 요청을 발행할 수 있는 Amazon DataZone HTTPS API를 사용하여 DataZone 프로그래밍 방식으로 Amazon에 액세스할 수 있습니다. 자세한 내용은 Amazon DataZone API 참조를 참조하십시오.

아마존 DataZone 용어 및 개념

Amazon을 시작할 때는 DataZone Amazon의 주요 개념, 용어 및 구성 요소를 이해하는 것이 중요합니다.

주제

아마존 DataZone 컴포넌트

Amazon은 다음과 같은 네 가지 주요 구성 요소를 DataZone 포함합니다.

- 비즈니스 데이터 카탈로그 - 이 구성 요소를 사용하여 비즈니스 컨텍스트와 함께 조직 전체의 데이터를 카탈로그화하여 조직의 모든 사람이 데이터를 빠르게 찾고 이해할 수 있도록 할 수 있습니다.
- 워크플로 게시 및 구독 - 이러한 자동화된 워크플로를 사용하여 셀프 서비스 방식으로 생산자와 소비자 간의 데이터를 보호하고 조직의 모든 사람이 올바른 목적에 맞는 올바른 데이터에 액세스할 수 있도록 할 수 있습니다.
- 프로젝트 및 환경
  - Amazon에서 DataZone 프로젝트는 분석에 대한 액세스를 단순화하는 데 사용되는 사람, 자산 (데이터) 및 도구를 그룹화하는 비즈니스 사용 사례를 기반으로 합니다. AWS 프로젝트는 프로젝트 구성원이 협업하고, 데이터를 교환하고, 자산을 공유할 수 있는 영역을 제공합니다. 기본적으로 프로젝트는 프로젝트에 명시적으로 추가된 사용자만 프로젝트 내의 데이터 및 분석 도구에 액세스할 수 있도록 구성됩니다. 프로젝트는 데이터 소비자가 액세스할 수 있도록 프로젝트 정책에 따라 생성된 자산의 소유권을 관리합니다.
  - Amazon DataZone 프로젝트 내에서 환경은 지정된 IAM 주체 세트 (예: 기여자 권한을 가진 사용자) 가 운영할 수 있는 0개 이상의 구성된 리소스 (예: Amazon S3 버킷, AWS Glue 데이터베이스 또는 Amazon Athena 작업 그룹) 의 모음입니다.

- 데이터 포털 (AWS Management Console 외부) - 다양한 사용자가 셀프 서비스 방식으로 데이터를 카탈로그 작성, 검색, 관리, 공유 및 분석할 수 있는 브라우저 기반 웹 애플리케이션입니다. 데이터 포털은 IAM 자격 증명 또는 ID 공급자의 기존 자격 증명으로 사용자를 인증합니다. AWS IAM Identity Center

Amazon DataZone 도메인이란 무엇입니까?

Amazon DataZone 도메인을 사용하여 자산, 사용자 및 프로젝트를 구성할 수 있습니다. Amazon DataZone 도메인과 추가 AWS 계정을 연결하여 데이터 소스를 통합할 수 있습니다. 그런 다음 메타데이터 완전성과 품질을 개선하는 메타데이터 양식 및 용어집과 함께 이러한 데이터 소스의 자산을 도메인 카탈로그에 게시할 수 있습니다. 또한 이러한 자산을 검색 및 탐색하여 도메인에 게시된 데이터를 확인할 수 있습니다. 또한 프로젝트에 참여하여 다른 사용자와 협업하고, 자산을 구독하고, 프로젝트 환경을 사용하여 Amazon Athena 및 Amazon Redshift와 같은 분석 도구에 액세스할 수 있습니다. Amazon DataZone 도메인을 사용하면 기업용 단일 Amazon 도메인을 생성하든 사업부별로 여러 Amazon DataZone DataZone 도메인을 생성하든 관계없이 조직 구조의 데이터 및 분석 요구 사항을 유연하게 반영할 수 있습니다.

Amazon DataZone 프로젝트 및 환경이란 무엇입니까?

Amazon은 팀, 도구 및 데이터를 사용 사례별로 그룹화하여 팀과 분석 사용자가 프로젝트에서 협업할 수 DataZone 있도록 합니다.

- Amazon에서는 프로젝트를 통해 사용자 그룹이 Amazon DataZone 카탈로그의 데이터를 게시, 검색, 구독 및 사용하는 것과 관련된 다양한 비즈니스 사용 사례에 대해 협업할 수 있습니다. DataZone 프로젝트 구성원은 Amazon DataZone 카탈로그의 자산을 사용하고 하나 이상의 분석 워크플로를 사용하여 새 자산을 생성합니다. 프로젝트는 데이터 포털 내에서 다음 활동을 지원합니다.
  - 프로젝트 소유자는 소유자 및 기여자 권한이 있는 구성원을 추가할 수 있습니다.
  - 프로젝트 구성원은 SSO 사용자, SSO 그룹, IAM 사용자일 수 있습니다.
  - 프로젝트 구성원은 데이터 카탈로그의 자산에 대한 구독을 요청할 수 있습니다.

    프로젝트에 구독 승인이 제공됩니다.
- Amazon DataZone 프로젝트에서 환경이란 0개 이상의 구성된 리소스 (예: Amazon S3, AWS Glue 데이터베이스 또는 Amazon Athena 워크그룹) 로 구성된 모음으로, 해당 리소스를 운영할 수 있는 지정된 IAM 보안 주체 집합이 있습니다. 환경은 환경 생성을 위한 재사용 가능한 템플릿을 제공하는 사전 구성된 리소스 및 청사진 세트인 환경 프로필을 사용하여 생성됩니다. 환경 프로파일은 환경이 배포되는 지역 AWS 계정 또는 지역과 같은 설정을 정의합니다.

아마존 DataZone 블루프린트란 무엇입니까?

환경이 생성되는 블루프린트는 환경이 속한 프로젝트의 구성원이 Amazon 카탈로그의 자산을 사용할 때 사용할 수 있는 AWS 도구 및 서비스 (예: Amazon DataZone Redshift) 를 정의합니다. AWS Glue

DataZoneAmazon의 현재 릴리스에서는 다음과 같은 기본 블루프린트가 지원됩니다.

블루프린트 이름	설명	생성할 리소스
데이터 레이크 블루프린트	Amazon DataZone 프로젝트 구성원이 환경 내에서 Data Lake 생산자 및 소비자 서비스를 시작할 수 있도록 합니다. 이를 통해 Amazon DataZone 프로젝트 구성원은 Amazon Athena와 Lake Formation이 지원하는 다른 쿼리 엔진에서 Lake Formation이 관리하는 자산의 '읽기 전용' 사본에 직접 액세스할 수 있습니다. 프로듀서로서 Amazon DataZone 프로젝트 구성원은 Amazon Athena를 사용하여 새로운 LakeFormation 관리형 테이블을 생성하고 이를 Amazon 카탈로그에 게시할 수 있습니다. DataZone	Amazon Athena를 사용하여 Lake Formation 테이블을 생성하고 쿼리할 수 있는 기능을 사용자에게 제공합니다. Amazon Athena 워크그룹, '읽기 전용' Lake Formation 권한, '읽기 전용' IAM 권한이 있는 AWS Glue 데이터베이스, 프로젝트에서 관리하는 Amazon S3에 대한 액세스 권한이 있는 데이터베이스 AWS Glue Lake Formation 권한 '생성' 및 '부여' 권한, '읽기' 및 '쓰기' IAM 권한, 태깅이 포함된 AWS Glue ETL (추출, 변환 및 로드) 이 있는 데이터베이스
데이터 웨어하우스 청사진	소비자는 이 청사진을 통해 Amazon DataZone 프로젝트 구성원이 자체 Amazon Redshift 클러스터에 연결하여 원격 데이터 스토어를 쿼리하고 새 데이터 세트를 생성 및 저장할 수 있습니다.	Amazon Redshift 쿼리 편집기에 대한 액세스, Amazon DataZone 카탈로그에서 구독한 데이터 소스에 대한 '읽기' 액세스, 구성된 Amazon Redshift 클러스터에서 로컬 자산을 생성하는 기능. Amazon Redshift 쿼리 편집기에 액세스

블루프린트 이름	설명	생성할 리소스
	생산자는 이 청사진을 통해 Amazon DataZone 프로젝트 구성원이 자신의 Amazon Redshift 클러스터에 연결하여 원격 데이터 스토어를 쿼리하고, 새 데이터 세트를 생성하고, Amazon 카탈로그에 게시할 수 있습니다. DataZone	하고, Amazon DataZone 카탈로그에서 구독한 데이터 소스에 대한 '읽기' 액세스, 구성된 Amazon Redshift 클러스터에서 자산을 생성하고 게시할 수 있습니다.
아마존 세이지메이커 청사진	이 청사진은 데이터 생산자와 소비자가 Amazon으로 원활하게 전환하여 기계 학습 (ML) 프로젝트에서 SageMaker 협업하는 동시에 데이터 및 ML 자산에 대한 액세스 거버넌스를 적용할 수 있도록 도와줍니다. DataZone Amazon과 Amazon SageMaker 간의 새로운 통합 기능을 통해 데이터 소비자와 생산자는 인프라 설정 전반에서 ML 거버넌스를 간소화하고, 비즈니스 이니셔티브에 대해 협업하고, 데이터와 ML 자산을 쉽게 관리할 수 있습니다.	Amazon에서 데이터 및 ML 자산을 검색, 구독 및 게시할 수 있는 Amazon SageMaker 도메인을 생성할 수 DataZone 있습니다. 또한 구성된 대로 AWS Glue 데이터베이스 및 Lake Formation을 구독하고 게시할 수 있습니다.

Amazon DataZone 인벤토리 및 게시 워크플로란 무엇입니까?

프로젝트 인벤토리 자산 생성

DataZone Amazon을 사용하여 데이터를 카탈로그화하려면 먼저 데이터 (자산) 를 프로젝트 인벤토리로 Amazon에 가져와야 DataZone 합니다. 프로젝트용 인벤토리를 생성하면 해당 프로젝트 구성원만 자산을 검색할 수 있습니다. 명시적으로 게시되지 않는 한 모든 도메인 사용자가 검색/찾아보기에서 프로젝트 인벤토리 자산을 사용할 수 있는 것은 아닙니다. DataZoneAmazon의 현재 릴리스에서는 다음과 같은 방법으로 프로젝트 인벤토리에 자산을 추가할 수 있습니다.

- 데이터 포털을 통해 또는 Amazon DataZone API를 사용하여 데이터 소스를 생성하고 실행합니다. Amazon의 현재 릴리스에서는 AWS Glue 및 Amazon DataZone Redshift용 데이터 소스를 생성하고 실행할 수 있습니다. AWS Glue 또는 Amazon Redshift 데이터 소스를 생성 및 실행하면 선택한 프로젝트 인벤토리에 자산을 생성하고 소스 데이터베이스 테이블 또는 데이터 웨어하우스에서 해당 기술 메타데이터를 인벤토리로 Amazon으로 가져올 수 있습니다. DataZone
- API를 사용하면 사용 가능한 시스템 자산 유형 (AWS Glue, Amazon Redshift, Amazon S3 객체) 또는 사용자 지정 자산 유형에서 자산을 생성할 수 있습니다.
  - Amazon DataZone API를 사용하여 프로젝트 인벤토리에 사용자 지정 자산 유형을 생성합니다. 사용자 지정 자산 유형에는 ML 모델, 대시보드, 온프레미스 테이블 등이 포함될 수 있습니다.
  - Amazon DataZone API를 사용하여 이러한 사용자 지정 자산 유형에서 자산을 생성합니다.
- Amazon DataZone 데이터 포털을 사용하여 S3 객체의 자산을 수동으로 생성합니다.

프로젝트 인벤토리 자산 큐레이션 - 프로젝트 인벤토리를 생성한 후 데이터 소유자는 비즈니스 이름 (자산 및 스키마), 설명 (자산 및 스키마), Read Me, 용어집 용어 (자산 및 스키마), 메타데이터 양식을 추가하거나 업데이트하여 필요한 비즈니스 메타데이터로 인벤토리 자산을 관리할 수 있습니다. 데이터 포털이나 Amazon DataZone API를 사용하여 이 작업을 수행할 수 있습니다. 자산을 편집할 때마다 새 인벤토리 버전이 생성됩니다.

Amazon DataZone 카탈로그에 프로젝트 인벤토리 자산 게시

Amazon을 사용하여 데이터를 DataZone 카탈로그화하는 다음 단계는 프로젝트의 인벤토리 자산을 도메인 사용자가 검색할 수 있도록 하는 것입니다. 아마존 DataZone 카탈로그에 인벤토리 자산을 게시하여 이 작업을 수행할 수 있습니다. 인벤토리 자산의 최신 버전만 카탈로그에 게시할 수 있으며 가장 최근에 게시된 버전만 검색 카탈로그에서 활성화됩니다. 재고 자산이 아마존 DataZone 카탈로그에 게시된 후 업데이트되는 경우, 검색 카탈로그에 최신 버전이 포함되도록 하려면 이를 다시 명시적으로 게시해야 합니다. DataZoneAmazon의 현재 릴리스에서는 다음과 같은 방법으로 프로젝트 인벤토리 자산을 Amazon DataZone 카탈로그에 게시할 수 있습니다.

- 데이터 포털을 통해 또는 Amazon DataZone API를 사용하여 프로젝트 인벤토리 자산을 Amazon DataZone 카탈로그에 수동으로 게시하십시오.
- 데이터 소스를 생성 또는 편집하는 과정에서 옵션으로 AWS Glue 자산을 카탈로그에 게시 또는 Amazon Redshift 자산을 카탈로그 설정에 게시하여 예약 또는 자동 데이터 소스 실행 중에 사용할 수 있도록 활성화하십시오. 이 설정을 활성화하면 데이터 소스 실행이 프로젝트 인벤토리에 자산을 추가한 다음 인벤토리 자산을 Amazon DataZone 카탈로그에 게시합니다. 직접 게시하는 경우 자산에 비즈니스 메타데이터가 없을 수 있으며 모든 도메인 사용자가 직접 검색할 수 있게 됩니다. 이 설

정은 데이터 포털을 통해 또는 Amazon DataZone API를 사용하여 데이터 소스에서 사용할 수 있습니다.

Amazon DataZone 구독 및 주문 처리 워크플로란 무엇입니까?

자산이 Amazon DataZone 카탈로그에 게시되면 도메인 사용자는 이러한 자산을 검색하고, 해당 자산에 대한 액세스를 요청 및 획득하고, DataZone Amazon을 계속 사용하여 이러한 자산을 관리, 공유 및 분석할 수 있습니다.

사용자는 프로젝트를 대신하여 해당 자산을 구독하여 자산에 대한 액세스를 요청합니다. 구독 요청이 생성되면 자산 소유자가 알림을 받고 구독 요청을 검토하고 승인 또는 거부 여부를 결정할 수 있습니다. 데이터 소유자가 구독 요청을 승인하면 구독 프로젝트에 해당 자산에 대한 액세스 권한이 부여됩니다.

구독 요청이 승인되면 Amazon은 AWS Lake Formation 또는 Amazon Redshift에서 필요한 지원금을 생성하여 프로젝트 내 모든 해당 환경에 자산을 자동으로 추가하는 구독 처리 워크플로를 DataZone 시작합니다. 이를 통해 구독하는 프로젝트 구성원은 자신의 환경에서 쿼리 도구 (Amazon Athena 또는 Amazon Redshift 쿼리 편집기) 중 하나를 사용하여 자산을 쿼리할 수 있습니다.

Amazon은 관리 자산 (AWS Glue 테이블 및 Amazon Redshift 테이블 및 보기 포함) 에 대해서만 이 자동 주문 처리 로직을 트리거할 DataZone 수 있습니다. 다른 모든 자산 유형 (비관리 자산) 의 경우 Amazon은 자동으로 주문 처리를 DataZone 트리거할 수 없으며 대신 필요한 모든 세부 정보를 이벤트 페이로드에 포함하여 Amazon Eventbridge에 이벤트를 게시하므로 Amazon 외부에서 필요한 보조금을 생성할 수 있습니다. DataZone DataZone 또한 Amazon은 Amazon 외부에서 구독이 완료되면 구독 상태를 업데이트할 DataZone 수 있는 `updateSubscriptionStatus` API를 DataZone 제공하므로 Amazon은 프로젝트 구성원에게 자산 사용을 시작할 수 있음을 알릴 수 있습니다.

Amazon의 사용자 페르소나 DataZone

다음은 기본 Amazon DataZone 사용자 페르소나입니다.

- Amazon을 조직의 분석 DataZone 플랫폼으로 설정한 도메인 관리자

  Amazon의 DataZone 경우 도메인 관리자는 AWS 계정에 DataZone Amazon을 설치하고, Amazon DataZone 도메인을 생성하고, Amazon DataZone 도메인과의 AWS 계정 연결 및 ID 공급자 연결을 구성합니다. 또한 도메인 관리자는 AWS 조직 및 AWS 서비스 카탈로그와 같은 다른 서비스 콘솔을 사용하여 Amazon을 구성합니다. DataZone

- 분석 및 기계 학습 작업을 수행하는 Amazon의 주 사용자 DataZone (자산 게시자 및 구독자) 인 데이터 사용자

  데이터 사용자에는 데이터 자산을 생산하고 소비하는 데이터 분석 작업자, 데이터 과학자, 시스템 사용자가 포함됩니다. Amazon의 DataZone 경우 데이터 사용자는 프로젝트 및 환경을 생성 및 가입하고, 사전 구성된 분석 또는 기계 학습 도구를 사용하여 데이터 자산을 구독 및 사용하고, 출력 데이터 자산을 Amazon DataZone 도메인 카탈로그에 다시 게시하여 다른 사람과 공유합니다.
- 사용자 지정 인프라 템플릿을 구축하고 DataZone Amazon을 내부 카탈로그 또는 프로덕션 시스템과 통합하는 시스템 개발자

  Amazon의 관점에서 보면 시스템 개발자는 환경 공급자로서 환경 청사진 (인프라 템플릿) 또는 Infrastructure-As-Code CI/CD 파이프라인을 구축하고 DataZone, 환경 전반에서 데이터 자산을 홍보하기 위한 데이터 파이프라인, 내부 카탈로그와 통합하기 위한 카탈로그 동기화 및 구독 승인 처리 어댑터, 또는 필요한 경우 Amazon API와 내부 사용자 인터페이스 또는 프로덕션 시스템 간의 통합을 구축합니다. DataZone
- 조직 보안, 개인 정보 보호 및 기타 규정 준수 정책의 정의와 위험을 소유하고 조직에서 DataZone Amazon을 사용할 때 이러한 정의를 준수하는지 확인하는 데이터 거버넌스 책임자.

아마존 DataZone 용어

도메인

Amazon DataZone 도메인은 자산, 사용자 및 프로젝트를 함께 연결하는 조직 주체입니다. Amazon DataZone 도메인을 사용하면 기업을 위한 단일 Amazon 도메인을 생성하든, 여러 데이터 영역을 생성하든, 다른 사업부 또는 팀을 위한 DataZone 도메인을 생성하든 관계없이 조직 구조의 데이터 및 분석 요구 사항을 유연하게 반영할 수 있습니다.

관련 계정

AWS 계정을 Amazon DataZone 도메인과 연결하면 이러한 AWS 계정의 데이터를 Amazon DataZone 카탈로그에 게시하고 Amazon DataZone 프로젝트를 생성하여 여러 AWS 계정의 데이터를 사용할 수 있습니다. 계정 연결 요청은 Amazon DataZone 도메인을 소유한 AWS 계정에서만 시작할 수 있습니다. 계정 연결 요청은 초대된 AWS 계정의 관리자만 수락할 수 있습니다. AWS 계정이 Amazon DataZone 도메인과 연결되면 이 계정의 AWS Glue 카탈로그 및 Amazon Redshift와 같은 데이터 소스를 이 도메인에 등록할 수 있습니다. 또한 AWS 계정을 연결하면 Amazon DataZone 프로젝트 및 환경을 만들 수 있습니다.

는 하나 이상의 Amazon DataZone 도메인과 연결할 AWS 계정 수 있습니다.

데이터 소스

DataZoneAmazon에서는 데이터 소스를 사용하여 원본 데이터베이스 또는 데이터 웨어하우스에서 자산 (데이터) 의 기술 메타데이터를 DataZone Amazon으로 가져올 수 있습니다. Amazon의 현재 릴리스에서는 AWS Glue 및 Amazon DataZone Redshift용 데이터 소스를 생성하고 실행할 수 있습니다. 데이터 소스를 생성하면 DataZone Amazon과 소스 (AWS Glue Data Catalog 또는 Amazon Redshift Warehouse) 간에 연결을 설정하여 테이블 이름, 열 이름, 데이터 유형을 비롯한 기술 메타데이터를 읽을 수 있습니다. 데이터 소스를 생성하면 DataZone Amazon에서 새 자산을 생성하거나 기존 자산을 업데이트하는 초기 데이터 소스 실행도 시작할 수 있습니다. 데이터 소스를 생성하는 동안 또는 데이터 소스를 성공적으로 생성한 후에 데이터 소스 실행 일정을 지정할 수도 있습니다.

데이터 원본 실행

DataZoneAmazon에서 데이터 소스 실행은 프로젝트 인벤토리에 자산을 생성하고 선택적으로 프로젝트 인벤토리 자산을 Amazon DataZone 카탈로그에 게시하기 위해 Amazon이 DataZone 수행하는 작업입니다. 데이터 소스 실행을 자동화 (데이터 소스 최초 생성 시 시작) 하거나 예약 또는 수동으로 실행할 수 있습니다. 데이터 선택 기준을 사용하면 프로젝트 인벤토리 또는 Amazon DataZone 카탈로그에 수집할 기존 및 미래 데이터 세트와 해당 인벤토리 또는 카탈로그 자산에 대한 메타데이터 업데이트 빈도를 세밀하게 조정할 수 있습니다.

구독 목표

DataZoneAmazon에서는 구독 대상을 통해 프로젝트에서 구독한 데이터에 액세스할 수 있습니다. 구독 대상은 Amazon DataZone 프로젝트 구성원이 구독한 데이터에 대한 쿼리를 시작할 수 있도록 Amazon이 원본 데이터와의 연결을 설정하고 필요한 권한을 생성하는 데 사용할 DataZone 수 있는 위치 (예: 데이터베이스 또는 스키마) 와 필요한 권한 (예: IAM 역할) 을 지정합니다.

구독 요청

DataZoneAmazon에서 구독 요청은 특정 자산에 대한 액세스 권한을 부여받기 위해 Amazon DataZone 프로젝트가 따라야 하는 프로세스입니다. 구독 요청은 승인, 거부, 취소 또는 승인될 수 있습니다.

자산

Amazon에서 자산은 단일 물리적 데이터 객체 (예: 테이블 DataZone, 대시보드, 파일) 또는 가상 데이터 객체 (예: 뷰) 를 제공하는 엔티티입니다.

애셋 유형

자산 유형은 자산이 Amazon DataZone 카탈로그에 표시되는 방식을 정의합니다. 자산 유형은 특정 유형의 자산에 대한 스키마를 정의합니다. 자산이 생성되면 자산 유형 (기본적으로 최신 버전) 에 정의된 스키마를 기준으로 자산의 유효성이 검사됩니다. 자산 업데이트가 발생하면 Amazon은 새

자산 버전을 DataZone 생성하여 Amazon DataZone 사용자가 모든 자산 버전을 운영할 수 있도록 합니다.

비즈니스 용어집

DataZoneAmazon에서 비즈니스 용어집은 자산과 연관될 수 있는 비즈니스 용어 모음입니다. 비즈니스 용어집은 조직의 다양한 데이터 분석 작업 전반에 걸쳐 동일한 용어와 정의를 사용하는 데 도움이 됩니다.

비즈니스 용어집의 용어를 자산 및 열에 추가하여 검색 중에 해당 속성을 분류하거나 식별성을 높일 수 있습니다. 자산과 연결된 메타데이터 양식에서 필드의 값 유형으로 용어집을 선택할 수 있습니다. 자산의 메타데이터 양식 필드 값으로 특정 용어를 선택하면 사용자는 비즈니스 용어집 용어를 검색하고 관련 자산을 찾을 수 있습니다.

메타데이터 양식 유형

메타데이터 양식 유형은 자산이 인벤토리로 생성되거나 Amazon DataZone 도메인에 게시될 때 수집 및 저장되는 메타데이터를 정의하는 템플릿입니다. 메타데이터 양식 유형을 데이터 자산과 연결할 수 있습니다. 메타데이터 양식 유형은 도메인 관리자가 규정 준수 정보, 규정 정보 또는 분류와 같은 해당 도메인에 필요한 메타데이터 양식을 정의하는 데 도움이 됩니다. 도메인 관리자는 이를 통해 자산에 대한 추가 메타데이터를 사용자 지정할 수 있습니다. DataZone Amazon에는 asset-common-details-form -type,,,,, column-business-metadata-form s3- object-collection-form-type subscription-terms-form-type, 및 glue-table-form-type 와 같은 시스템 메타데이터 양식 유형이 있습니다. glue-view-form-type redshift-table-form-type redshift-view-form-type suggestion-form-type

메타데이터 양식

DataZoneAmazon에서 메타데이터 양식은 자산을 인벤토리로 생성하거나 Amazon DataZone 도메인에 게시할 때 수집 및 저장되는 메타데이터를 정의합니다. 메타데이터 양식 정의는 도메인 관리자가 카탈로그 도메인에서 생성합니다. 메타데이터 양식 정의는 부울, 날짜, 십진수, 정수, 문자열 및 비즈니스 용어집 필드 값 데이터 유형을 지원하는 하나 이상의 필드 정의로 구성됩니다.

도메인 관리자는 도메인에 메타데이터 양식을 추가하여 해당 도메인의 자산에 메타데이터 양식을 적용합니다. 그런 다음 에셋 퍼블리셔는 메타데이터 양식에 선택 및 필수 필드 값을 제공합니다.

프로젝트

Amazon에서는 사용자 그룹이 프로젝트를 통해 프로젝트 인벤토리에 자산을 생성하여 모든 프로젝트 구성원이 자산을 검색할 수 있도록 한 다음 Amazon 카탈로그에 자산을 게시 DataZone, 검색, 구독 및 소비하는 등 다양한 비즈니스 사용 사례에 대해 협업할 수 있습니다. DataZone 프로젝트 구성원은 Amazon DataZone 카탈로그의 자산을 사용하고 하나 이상의 분석 워크플로를 사용하여 새 자산을 생성합니다. 프로젝트 구성원은 소유자 또는 기여자일 수 있습니다. 프로젝트 소유자는 다

른 사용자를 소유자 또는 기여자로 추가하거나 제거할 수 있으며 프로젝트를 수정하거나 삭제할 수 있습니다. 기여자에 대한 기타 제한은 정책으로 정의할 수 있습니다. 사용자가 프로젝트를 만들면 해당 프로젝트의 첫 번째 소유자가 됩니다.

환경

환경은 구성된 리소스 (예: Amazon S3 버킷, AWS Glue 데이터베이스 또는 Amazon Athena 작업 그룹) 의 모음으로, 해당 리소스를 운영할 수 있는 지정된 IAM 보안 주체 세트 (기여자 권한이 할당됨) 가 있습니다. 또한 각 환경에는 리소스에 액세스하고 구독 및 주문 처리를 통해 데이터에 액세스할 권한이 있는 사용자 주체가 있을 수 있습니다. 환경은 AWS 서비스와 외부 IDE 및 콘솔에 대한 실행 가능한 링크를 저장하도록 설계되었습니다. 프로젝트 구성원은 환경 내에 구성된 딥 링크를 통해 Amazon Athena 콘솔 등과 같은 서비스에 액세스할 수 있습니다. 프로젝트의 SSO 사용자 및 IAM 사용자는 특정 환경을 사용하거나 액세스할 수 있도록 범위를 더 좁힐 수 있습니다.

환경 프로필

DataZoneAmazon에서 환경 프로파일은 환경을 생성하는 데 사용할 수 있는 템플릿입니다. 환경 프로파일은 블루프린트를 사용하여 생성됩니다.

환경 프로필을 사용하면 도메인 관리자가 사전 구성된 매개 변수로 청사진을 래핑한 다음 데이터 작업자는 기존 환경 프로필을 선택하고 새 환경의 이름을 지정하여 새 환경을 원하는 수만큼 빠르게 만들 수 있습니다. 이를 통해 데이터 작업자는 도메인 관리자가 시행하는 데이터 거버넌스 정책을 준수하면서 프로젝트와 환경을 효율적으로 관리할 수 있습니다.

청사진

환경이 생성되는 블루프린트는 환경이 속한 프로젝트의 구성원이 Amazon 카탈로그의 자산을 사용할 때 사용할 수 있는 AWS 도구 및 서비스 (예: Amazon DataZone Redshift) 를 정의합니다. AWS Glue

DataZone Amazon의 현재 릴리스에서는 다음과 같은 기본 블루프린트가 지원됩니다.

- 데이터 레이크 블루프린트
- 데이터 웨어하우스 청사진
- 아마존 세이지메이커 청사진

사용자 프로필

사용자 프로필은 Amazon DataZone 사용자를 나타냅니다. Amazon은 다양한 목적으로 Amazon DataZone 관리 콘솔 및 데이터 포털과 상호 작용할 수 있도록 IAM 역할과 SSO ID를 모두 DataZone 지원합니다. 도메인 관리자는 IAM 역할을 사용하여 Amazon DataZone Management Console에서 새 Amazon 도메인 생성, 메타데이터 양식 유형 구성, 정책 구현 등 DataZone 도메인

관련 초기 관리 작업을 수행합니다. 데이터 작업자는 Identity Center를 통해 SSO 기업 ID를 사용하여 Amazon DataZone Data Portal에 로그인하고 멤버십이 있는 프로젝트에 액세스합니다.

그룹 프로필

그룹 프로필은 Amazon DataZone 사용자 그룹을 나타냅니다. 그룹을 수동으로 만들거나 기업 고객의 Active Directory 그룹에 매핑할 수 있습니다. DataZoneAmazon에서 그룹은 두 가지 용도로 사용됩니다. 첫째, 그룹을 조직도의 사용자 팀에 매핑할 수 있으므로 팀에 새로 합류하거나 퇴사하는 직원이 있을 때 Amazon DataZone 프로젝트 소유자의 관리 업무를 줄일 수 있습니다. 둘째, 기업 관리자는 Active Directory 그룹을 사용하여 사용자 상태를 관리하고 업데이트하므로 Amazon DataZone 도메인 관리자는 이러한 그룹 멤버십을 사용하여 Amazon DataZone 도메인 정책을 구현할 수 있습니다.

도메인 관리자

DataZoneAmazon에서는 Amazon 도메인을 생성하는 IAM 보안 주체가 해당 DataZone 도메인의 기본 도메인 관리자입니다. Amazon의 도메인 관리자는 도메인 생성, 다른 도메인 관리자 할당, 데이터 소스 및 구독 대상 추가, 프로젝트 및 환경 생성, 프로젝트 소유자 할당 등 도메인의 주요 기능을 DataZone 수행합니다.

퍼블리셔

DataZoneAmazon에서는 게시자가 자산을 Amazon DataZone 카탈로그에 게시하고 게시한 자산의 메타데이터를 편집할 수 있습니다. 이 권한이 부여되면 게시자는 아마존 카탈로그에 게시한 자산에 대한 구독 요청을 승인하거나 거부할 수 있습니다. DataZone

구독자

DataZoneAmazon에서 구독자는 Amazon 카탈로그에서 자산을 찾고, 액세스하고, 사용하려는 Amazon DataZone DataZone 프로젝트입니다.

AWS 계정 owner

DataZoneAmazon에서는 AWS 계정 소유자가 자신의 역할, 정책 및 권한을 생성하여 Amazon DataZone 도메인과 AWS 계정 연결할 수 AWS 계정 있도록 합니다.

아마존의 새로운 점은 무엇입니까 DataZone?

이 섹션에서는 출시 DataZone 날짜별로 Amazon의 새로운 기능과 개선 사항을 설명합니다.

주제

2024년

아마존 DataZone , 아마존과의 통합 시작 SageMaker

2024년 5월 6일에 출시되었습니다.

Amazon은 SageMakerAmazon과의 통합을 DataZone 시작하여 데이터 생산자와 소비자가 Amazon으로 원활하게 전환하여 기계 학습 (ML) 프로젝트에서 SageMaker 협업하는 동시에 데이터 및 ML 자산에 대한 액세스 거버넌스를 적용할 수 있도록 지원합니다. DataZone Amazon과 Amazon SageMaker 간의 새로운 통합 기능을 통해 데이터 소비자와 생산자는 인프라 설정 전반에서 ML 거버넌스를 간소화하고, 비즈니스 이니셔티브에 대해 협업하고, 데이터와 ML 자산을 쉽게 관리할 수 있습니다. 자세한 내용은 Amazon DataZone 내장 블루프린트로 작업하기 및 관련 계정을 사용하여 데이터 게시 및 사용 섹션을 참조하세요.

아마존 DataZone , AWS Lake Formation 하이브리드 액세스 모드와의 통합 출시

2024년 4월 3일에 출시되었습니다.

DataZone Amazon은 AWS Lake Formation 하이브리드 액세스 모드와의 통합을 도입했습니다. 이 통합을 통해 AWS Lake Formation에 먼저 등록할 필요 없이 DataZone Amazon을 통해 AWS Glue 테이블을 쉽게 게시하고 공유할 수 있습니다. 시작하려면 관리자가 Amazon DataZone 콘솔의 `DefaultDataLake` 블루프린트에서 데이터 위치 등록 설정을 활성화해야 합니다. 그런 다음 데이터 소비자가 IAM 권한을 통해 관리되는 AWS Glue 테이블을 구독하면 Amazon은 DataZone 먼저 하이브리드 모드에서 이 테이블의 Amazon S3 위치를 등록한 다음 Lake AWS Formation을 통해 테이블에 대한 권한을 관리하여 데이터 소비자에게 액세스 권한을 부여합니다. 이렇게 하면 기존 워크플로에 영향을 주지 않으면서 테이블에 대한 IAM 권한이 새로 부여된 AWS Lake Formation 권한으로 계속 존재할

수 있습니다. 자세한 내용은 아마존과 AWS 레이크 포메이션 하이브리드 모드 DataZone 통합 을 참조하세요.

아마존 DataZone , AWS Glue Data Quality와의 통합 시작

2024년 4월 3일에 출시되었습니다.

Amazon은 AWS Glue Data Quality와의 통합을 DataZone 시작하고 타사 데이터 품질 솔루션의 데이터 품질 지표를 통합하는 API를 제공합니다. 새로운 통합을 통해 AWS Glue Data Quality 점수를 Amazon DataZone 비즈니스 데이터 카탈로그에 자동으로 게시할 수 있습니다. Amazon DataZone API는 타사 소스의 품질 지표를 수집하는 데 사용할 수 있습니다. 게시되면 데이터 소비자는 데이터 자산을 쉽게 검색하고, 세분화된 품질 지표를 보고, 실패한 검사 및 규칙을 식별하여 비즈니스 의사 결정을 내릴 수 있습니다. 자세한 내용은 아마존의 데이터 품질 DataZone을 참조하세요.

Amazon 내 설명에 대한 AI 권장 사항의 일반 출시 DataZone

2024년 3월 27일에 출시되었습니다.

Amazon은 비즈니스 데이터 카탈로그를 강화하여 데이터 검색, 데이터 이해 및 데이터 사용을 개선할 수 있는 새로운 제너레이티브 AI 기반 기능의 정식 출시 DataZone 소식을 발표했습니다. 데이터 생산자는 클릭 한 번으로 포괄적인 비즈니스 데이터 설명 및 컨텍스트를 생성하고, 영향력 있는 열을 강조 표시하고, 분석 사용 사례에 대한 권장 사항을 포함할 수 있습니다. 이번 출시에는 데이터 생산자가 자산에 대한 설명을 프로그래밍 방식으로 생성하는 데 사용할 수 있는 API에 대한 지원이 추가되었습니다. 자세한 정보는 머신 러닝 및 제너레이티브 AI 사용을 참조하세요.

Amazon DataZone , Amazon Redshift 통합 개선 사항 출시

2024년 3월 21일에 출시되었습니다.

DataZone 아마존은 Amazon Redshift 테이블 및 뷰를 게시하고 구독하는 프로세스를 간소화하는 Amazon Redshift 통합에 몇 가지 개선 사항을 도입했습니다. 이러한 업데이트는 데이터 생산자와 소비자 모두의 경험을 간소화하여 Amazon DataZone 관리자가 제공하는 사전 구성된 자격 증명과 연결 매개변수를 사용하여 데이터 웨어하우스 환경을 빠르게 만들 수 있도록 합니다. 또한 이러한 개선 사항을 통해 관리자는 자신의 AWS 계정과 Amazon Redshift 클러스터 내에서 누가 어떤 목적으로 리소스를 사용할 수 있는지 더 잘 제어할 수 있습니다.

- 블루프린트 구성: 블루프린트를 활성화하면 활성화된 `DefaultDataWarehouseBlueprint` 블루프린트에 관리 프로젝트를 할당하여 계정에서 `DefaultDataWarehouseBlueprint` 블루프린트를 사용하여 환경 프로필을 생성할 수 있는 프로젝트를 제어할 수 있습니다. 클러스터, 데이터베이스, 시크릿 등의 파라미터를 `DefaultDataWarehouseBlueprint` 제공하여 그 위에 파라미터 세

트를 생성할 수도 있습니다. AWS Amazon DataZone 콘솔 내에서 AWS 시크릿을 생성할 수도 있습니다.

- 환경 프로필: 환경 프로필을 생성할 때 Amazon Redshift 파라미터를 직접 제공하거나 블루프린트 구성의 파라미터 세트 중 하나를 사용할 수 있습니다. 블루프린트 구성에서 생성한 파라미터 세트를 사용하기로 선택한 경우, AWS 시크릿에는 `AmazonDataZoneDomain` 태그만 필요합니다 (환경 프로파일에 자체 파라미터 세트를 제공하기로 선택한 경우에만 `AmazonDataZoneProject` 태그가 필요합니다). 환경 프로파일에서 승인된 프로젝트 목록을 지정할 수 있습니다. 승인된 프로젝트만 이 환경 프로필을 사용하여 데이터 웨어하우스 환경을 만들 수 있습니다. 또한 어떤 데이터 인증 프로젝트를 게시할 수 있는지 지정할 수 있습니다. 현재 다음 옵션 중 하나를 선택할 수 있습니다. 1) 모든 스키마에서 게시, 2) 기본 환경 스키마에서 게시, 3) 게시 허용 안 함.
- 환경: 이제 데이터 생산자 또는 소비자는 AWS 보안, 클러스터, 작업 그룹 및 데이터베이스를 비롯한 자체 Amazon Redshift 파라미터를 제공할 필요 없이 환경 프로필을 선택하여 환경을 만들 수 있습니다. 이러한 파라미터는 환경 프로파일에서 환경으로 포팅됩니다. Amazon은 환경 생성과 함께 DataZone 이제 환경에 대한 기본 스키마도 생성합니다. 프로젝트 구성원은 이 스키마에 대한 읽기 및 쓰기 액세스 권한을 가지며 환경 생성의 일환으로 생성된 기본 데이터 소스를 실행하여 이 스키마에서 생성된 테이블을 카탈로그에 쉽게 게시할 수 있습니다. 환경을 생성하는 데 사용되는 Amazon Redshift 파라미터를 사용하여 새 데이터 소스를 생성할 수도 있습니다 (데이터 생산자가 데이터 소스 생성 시 자체 파라미터를 제공하는 대신).

AWS Amazon을 위한 클라우드 구성 지원 DataZone

2024년 1월 18일에 출시되었습니다.

Amazon 사용자는 이제 Amazon DataZone 리소스 제품군을 효과적으로 모델링하고 관리하는 AWS CloudFormation 데 활용할 DataZone 수 있습니다. 이 접근 방식은 일관된 리소스 프로비저닝을 촉진하는 동시에 코드형 인프라 프랙티스를 통해 수명 주기 관리를 가능하게 합니다. 사용자 지정 템플릿을 사용하면 필요한 리소스와 상호 종속성을 정확하게 정의할 수 있습니다. 자세한 내용은 Amazon DataZone 리소스 유형 참조를 참조하십시오.

IAM 보안 주체를 Amazon 프로젝트의 구성원으로 직접 추가 DataZone

2024년 1월 5일에 출시되었습니다.

이제 IAM 보안 주체가 아직 Amazon에 로그인하지 않았더라도 (이전 요구 사항) IAM 보안 주체를 프로젝트 구성원으로 추가할 수 있습니다. DataZone 도메인 관리자 또는 IT 관리자가 도메인의 도메인 실행 역할을 `iam:GetUser` 추가한 후, 프로젝트 소유자는 IAM 역할 또는 IAM 사용자의 Amazon Resource Name (ARN) 을 제공하기만 하면 IAM 보안 주체를 구성원으로 추가할 수 있습니

다. `iam:GetRole` IAM 보안 주체는 여전히 Amazon에 액세스하는 데 필요한 IAM 권한을 가지고 있어야 DataZone 하며 이러한 권한은 IAM 콘솔에서 구성할 수 있습니다. 자세한 정보는 프로젝트에 구성원 추가을 참조하세요.

데이터 포털의 사용자 지정 자산 유형 지원

2024년 1월 5일에 출시되었습니다.

사용자 지정 자산이 지원되므로 DataZone Amazon은 Data Portal을 통해 대시보드, 쿼리, 모델 등의 비정형 데이터에 대한 자산을 카탈로그화할 수 있으므로 이전에 제공되었던 API 지원과 함께 데이터 포털에서 직접 사용자 지정 자산을 더 쉽게 추가할 수 있습니다. DataZoneAmazon에서 사용자 지정 자산을 생성, 업데이트 및 게시할 수 있으므로 모든 유형의 자산을 공유, 검색, 구독하고 해당 자산에 대한 거버넌스를 제공하는 비즈니스 워크플로를 구축할 수 있습니다. 자세한 정보는 사용자 지정 자산 유형 생성을 참조하세요.

2023년

도메인 삭제

2023년 12월 27일에 출시되었습니다

도메인을 더 쉽게 삭제할 수 있는 기능입니다. 이제 비어 있지 않아도 도메인 삭제를 진행할 수 있습니다 (예: 프로젝트, 환경, 자산, 데이터 원본 등이 포함된 경우). 자세한 정보는 도메인 삭제을 참조하세요.

하이브리드 모드

2023년 12월 22일에 출시되었습니다

DataZone Amazon은 AWS Lake Formation 하이브리드 모드에 대한 지원을 추가했습니다. 이 지원을 통해 하이브리드 모드에서 Lake Formation에 AWS S3 위치가 등록된 상태로 AWS Glue 테이블을 DataZone Amazon에 게시하면 Amazon은 이 테이블을 관리 자산으로 DataZone 취급하고 이 테이블에 대한 구독 허가를 관리할 수 있습니다. 이 기능이 출시되기 전에 Amazon은 DataZone 이 테이블을 비관리 자산으로 취급했습니다. 즉, DataZone Amazon은 이 테이블에 대한 구독을 승인할 수 없었습니다. 자세한 정보는 Amazon에 대한 Lake Formation 권한 구성 DataZone을 참조하세요.

HIPAA 자격 획득

2023년 12월 14일에 출시되었습니다.

DataZone Amazon은 현재 1996년 미국 건강 보험 양도 및 책임법 (HIPAA) 을 준수하고 있습니다. HIPAA 규정을 준수하는 AWS 서비스 목록을 보려면 https://aws.amazon.com/compliance/ /을 참조하십시오. hipaa-eligible-services-reference

Amazon 설명에 대한 AI 권장 사항 DataZone (미리 보기)

2023년 11월 28일에 출시되었습니다.

AWS 비즈니스 데이터 카탈로그를 보강하여 데이터 검색, 데이터 이해 및 데이터 사용을 개선할 수 DataZone 있는 Amazon의 새로운 제너레이티브 AI 기반 기능의 미리보기를 발표합니다. 데이터 생산자는 클릭 한 번으로 포괄적인 비즈니스 데이터 설명 및 컨텍스트를 생성하고, 영향력 있는 열을 강조 표시하고, 분석 사용 사례에 대한 권장 사항을 포함할 수 있습니다. DataZoneAmazon의 설명에 대한 AI 권장 사항을 통해 데이터 소비자는 분석에 필요한 데이터 테이블과 열을 식별할 수 있으므로 데이터 검색 가능성이 향상되고 데이터 생산자와의 back-and-forth 커뮤니케이션이 줄어듭니다. 미리 보기는 미국 동부 (버지니아 북부), 미국 서부 (오레곤) AWS 지역에서 프로비저닝된 Amazon DataZone 도메인에서 사용할 수 있습니다. 자세한 정보는 머신 러닝 및 제너레이티브 AI 사용을 참조하세요.

DefaultDataLake 청사진 개선

2023년 11월 20일에 출시되었습니다.

DataZone Amazon은 누가 귀하의 AWS 계정에서 어떤 데이터를 게시할 수 있는지 더 잘 제어할 수 있도록 DefaultDataLake 청사진에 개선 사항을 추가했습니다. 이번 기능 출시와 함께 도입된 두 가지 주요 변경 사항이 있습니다.

- 콘솔에서 블루프린트를 활성화하면 활성화된 DefaultDataLake 블루프린트에 프로젝트 관리를 할당하여 계정의 DefaultDataLake 블루프린트를 사용하여 환경 프로필을 만들 수 있는 프로젝트를 제어할 수 있습니다.
- 두 번째 변경사항은 포털에 있습니다. DefaultDataLake 블루프린트를 사용하여 환경 프로필을 만드는 경우 환경 생성에 환경 프로필을 사용할 수 있는 승인된 프로젝트를 선택할 수도 있습니다. 기본적으로 모든 프로젝트에서 데이터 레이크 환경 프로필을 사용할 수 있지만 환경 프로필을 특정 프로젝트로 제한하고 프로필로 만든 환경을 사용하여 게시할 수 있는 데이터를 제어할 수도 있습니다.

자세한 내용은 환경 프로필 생성을(를) 참조하세요.

설정

DataZoneAmazon을 설정하려면 AWS 계정이 있어야 하며 DataZone Amazon에 필요한 IAM 정책 및 권한을 설정해야 합니다.

Amazon DataZone 권한을 설정한 후에는 Amazon DataZone 도메인 생성, 데이터 포털 URL 획득, 데이터 생산자 및 데이터 소비자를 위한 기본 Amazon DataZone 워크플로를 안내하는 시작하기 섹션의 단계를 완료하는 것이 좋습니다.

주제

- AWS 계정을 등록하세요.
- Amazon DataZone 관리 콘솔을 사용하는 데 필요한 IAM 권한을 구성합니다.
- Amazon DataZone 데이터 포털을 사용하는 데 필요한 IAM 권한을 구성합니다.
- 아마존용 AWS IAM 아이덴티티 센터 설정 DataZone

AWS 계정을 등록하세요.

계정이 없는 경우 다음 단계를 완료하여 AWS 계정을 만드십시오.

AWS 조직이 있는 경우 계정을 만드세요.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/organizations/ 에서 Organizations 콘솔을 엽니다.
2. 탐색 창에서 AWS 계정을 선택합니다.
3. AWS 계정 추가를 선택합니다.
4. AWS 계정 생성을 선택하고 요청된 세부 정보를 제공합니다. AWS 계정 생성을 선택합니다.

AWS 계정을 등록하려면

1. https://portal.aws.amazon.com/billing/signup을 엽니다.
2. 온라인 지시 사항을 따르세요.

   등록 절차 중에는 전화를 받고 키패드로 인증 코드를 입력하는 과정이 있습니다.

계정을 등록하면 AWS AWS 계정 루트 사용자가 생성됩니다. 루트 사용자는 계정의 모든 AWS 서비스와 리소스에 액세스할 수 있습니다. 보안 모범 사례는 관리 사용자에게 관리자 액세스 권한을 할당하고, 오직 루트 사용자만 루트 사용자 액세스 권한이 필요한 태스크를 수행하는 것입니다.

Amazon DataZone 관리 콘솔을 사용하는 데 필요한 IAM 권한을 구성합니다.

Amazon DataZone 관리 콘솔을 사용하려는 모든 사용자, 그룹 또는 역할에는 필요한 권한이 있어야 합니다.

주제

- Amazon DataZone 콘솔 액세스를 위해 사용자, 그룹 또는 역할에 필수 및 선택적 정책 첨부
- Amazon DataZone 서비스 콘솔의 간소화된 역할 생성을 활성화하기 위해 IAM 권한에 대한 사용자 지정 정책을 생성합니다.
- Amazon DataZone 도메인과 연결된 계정을 관리할 수 있는 권한에 대한 사용자 지정 정책을 생성합니다.
- (선택 사항) AWS Identity Center 권한에 대한 사용자 지정 정책을 생성하여 도메인에 SSO (Single Sign-On) 를 활성화하세요.
- (선택 사항) Amazon DataZone 도메인에 대한 SSO 사용자 및 SSO 그룹 액세스를 추가 및 제거하기 위한 AWS ID 센터 권한에 대한 사용자 지정 정책을 생성합니다.
- (선택 사항) IAM 보안 주체를 키 사용자로 추가하여 KMS (키 관리 서비스) 의 고객 관리 AWS 키로 Amazon DataZone 도메인을 생성합니다.

Amazon DataZone 콘솔 액세스를 위해 사용자, 그룹 또는 역할에 필수 및 선택적 정책 첨부

필수 및 선택적 사용자 지정 정책을 사용자, 그룹 또는 역할에 첨부하려면 다음 절차를 완료하십시오. 자세한 정보는 AWS 아마존 관리형 정책 DataZone을 참조하세요.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/iam/ 에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 정책을 선택합니다.
3. 다음 정책을 선택하여 사용자, 그룹 또는 역할에 연결하십시오.

- 정책 목록에서 옆의 확인란을 선택합니다 AmazonDataZoneFullAccess. [Filter] 메뉴와 검색 상자를 사용하여 정책 목록을 필터링할 수 있습니다. 자세한 정보는 AWS 관리형 정책: AmazonDataZoneFullAccess을 참조하세요.
- (선택 사항) Amazon DataZone 서비스 콘솔에서 역할 생성을 단순화할 수 있도록 IAM 권한에 대한 사용자 지정 정책을 생성합니다.
- (선택 사항) AWS ID 센터 권한에 대한 사용자 지정 정책을 생성하여 도메인에 SSO (Single Sign-On) 를 활성화하십시오.
- (선택 사항) Amazon DataZone 도메인에 대한 SSO 사용자 및 SSO 그룹 액세스를 추가 및 제거하기 위한 AWS ID 센터 권한에 대한 사용자 지정 정책을 생성합니다.

4. 작업(Actions)을 선택한 후 연결(Attach)을 선택합니다.
5. 정책을 연결할 사용자, 그룹 또는 역할을 선택합니다. 필터 메뉴와 검색 상자를 사용하면 보안 주체 개체 목록을 필터링할 수 있습니다. 사용자, 그룹 또는 역할을 선택한 후 정책 연결을 선택합니다.

Amazon DataZone 서비스 콘솔의 간소화된 역할 생성을 활성화하기 위해 IAM 권한에 대한 사용자 지정 정책을 생성합니다.

다음 절차를 완료하여 Amazon이 사용자를 대신하여 AWS 관리 콘솔에서 필요한 역할을 생성할 수 있도록 필요한 권한을 DataZone 갖도록 사용자 지정 인라인 정책을 생성하십시오.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/iam/ 에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 사용자 또는 사용자 그룹을 선택합니다.
3. 목록에서 정책을 삽입할 사용자 또는 그룹 이름을 선택합니다.
4. 권한 탭을 선택하고 필요하다면 Permissions policies(권한 정책) 섹션을 확장합니다.
5. 권한 추가 및 인라인 정책 생성 링크를 선택합니다.
6. 정책 생성 화면의 정책 편집기 섹션에서 JSON을 선택합니다.

   다음 JSON 명령문을 사용하여 정책 문서를 생성한 후 다음을 선택합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Action": [
                "iam:CreatePolicy",
                "iam:CreateRole"
            ],
            "Resource": [
                "arn:aws:iam::*:policy/service-role/AmazonDataZone*",
                "arn:aws:iam::*:role/service-role/AmazonDataZone*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "iam:AttachRolePolicy",
            "Resource": "arn:aws:iam::*:role/service-role/AmazonDataZone*",
            "Condition": {
                "ArnLike": {
                    "iam:PolicyARN": [
                        "arn:aws:iam::aws:policy/AmazonDataZone*",
                        "arn:aws:iam::*:policy/service-role/AmazonDataZone*"
                    ]
                }
            }
        }
    ]
}
```

7. 정책 검토 화면에서 정책 이름을 입력합니다. 정책에 만족하면 정책 생성을 선택합니다. 화면 상단에 있는 빨간색 상자에 표시되는 오류가 있지 않은지 확인합니다. 표시되는 오류가 있다면 수정합니다.

Amazon DataZone 도메인과 연결된 계정을 관리할 수 있는 권한에 대한 사용자 지정 정책을 생성합니다.

다음 절차를 완료하여 도메인의 리소스 공유를 나열, 수락 및 거부하는 데 필요한 권한을 관련 AWS 계정에 부여한 다음 관련 계정에서 환경 블루프린트를 활성화, 구성 및 비활성화하는 데 필요한 권한을 부여하는 사용자 지정 인라인 정책을 생성합니다. 블루프린트 구성 중에 옵션으로 제공되는 Amazon DataZone 서비스 콘솔 간소화 역할 생성을 활성화하려면 반드시 활성화해야 합니다. Amazon DataZone 서비스 콘솔의 간소화된 역할 생성을 활성화하기 위해 IAM 권한에 대한 사용자 지정 정책을 생성합니다.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/iam/ 에서 IAM 콘솔을 엽니다.

2. 탐색 창에서 사용자 또는 사용자 그룹을 선택합니다.
3. 목록에서 정책을 삽입할 사용자 또는 그룹 이름을 선택합니다.
4. 권한 탭을 선택하고 필요하다면 Permissions policies(권한 정책) 섹션을 확장합니다.
5. 권한 추가 및 인라인 정책 생성 링크를 선택합니다.
6. 정책 생성 화면의 정책 편집기 섹션에서 JSON을 선택합니다. 다음 JSON 명령문을 사용하여 정책 문서를 생성한 후 다음을 선택합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "datazone:ListEnvironmentBlueprintConfigurations",
                "datazone:PutEnvironmentBlueprintConfiguration",
                "datazone:GetDomain",
                "datazone:ListDomains",
                "datazone:GetEnvironmentBlueprintConfiguration",
                "datazone:ListEnvironmentBlueprints",
                "datazone:GetEnvironmentBlueprint",
                "datazone:ListAccountEnvironments",
                "datazone:DeleteEnvironmentBlueprintConfiguration"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": [
                "arn:aws:iam::*:role/AmazonDataZone",
                "arn:aws:iam::*:role/service-role/AmazonDataZone*"
            ],
            "Condition": {
                "StringEquals": {
                    "iam:passedToService": "datazone.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
```

```
            "Action": "iam:AttachRolePolicy",
            "Resource": "arn:aws:iam::*:role/service-role/AmazonDataZone*",
            "Condition": {
                "ArnLike": {
                    "iam:PolicyARN": [
                        "arn:aws:iam::aws:policy/AmazonDataZone*",
                        "arn:aws:iam::*:policy/service-role/AmazonDataZone*"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "iam:ListRoles",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreatePolicy",
                "iam:CreateRole"
            ],
            "Resource": [
                "arn:aws:iam::*:policy/service-role/AmazonDataZone*",
                "arn:aws:iam::*:role/service-role/AmazonDataZone*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ram:AcceptResourceShareInvitation",
                "ram:RejectResourceShareInvitation",
                "ram:GetResourceShareInvitations"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "*"
```

```
        },
        {
            "Effect": "Allow",
            "Action": "s3:CreateBucket",
            "Resource": "arn:aws:s3:::amazon-datazone*"
        }
    ]
}
```

7. 정책 검토 화면에서 정책 이름을 입력합니다. 정책에 만족하면 정책 생성을 선택합니다. 화면 상단에 있는 빨간색 상자에 표시되는 오류가 있지 않은지 확인합니다. 표시되는 오류가 있다면 수정합니다.

(선택 사항) AWS Identity Center 권한에 대한 사용자 지정 정책을 생성하여 도메인에 SSO (Single Sign-On) 를 활성화하세요.

Amazon의 AWS IAM ID 센터를 사용하여 Single Sign-On (SSO) 을 활성화하는 데 필요한 권한을 갖도록 사용자 지정 인라인 정책을 생성하려면 다음 절차를 완료하십시오. DataZone

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/iam/ 에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 사용자 또는 사용자 그룹을 선택합니다.
3. 목록에서 정책을 삽입할 사용자 또는 그룹 이름을 선택합니다.
4. 권한 탭을 선택하고 필요하다면 Permissions policies(권한 정책) 섹션을 확장합니다.
5. 권한 추가 및 인라인 정책 생성을 선택합니다.
6. 정책 생성 화면의 정책 편집기 섹션에서 JSON을 선택합니다.

   다음 JSON 명령문을 사용하여 정책 문서를 생성한 후 다음을 선택합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso:DeleteManagedApplicationInstance",
                "sso:CreateManagedApplicationInstance",
                "sso:PutApplicationAssignmentConfiguration"
```

```
            ],
            "Resource": "*"
        }
    ]
}
```

7. 정책 검토 화면에서 정책 이름을 입력합니다. 정책에 만족하면 정책 생성을 선택합니다. 화면 상단에 있는 빨간색 상자에 표시되는 오류가 있지 않은지 확인합니다. 표시되는 오류가 있다면 수정합니다.

(선택 사항) Amazon DataZone 도메인에 대한 SSO 사용자 및 SSO 그룹 액세스를 추가 및 제거하기 위한 AWS ID 센터 권한에 대한 사용자 지정 정책을 생성합니다.

Amazon 도메인에 SSO 사용자 및 SSO 그룹 액세스를 추가 및 제거하는 데 필요한 권한을 갖도록 사용자 지정 인라인 정책을 생성하려면 다음 절차를 완료하십시오. DataZone

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/iam/ 에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 사용자 또는 사용자 그룹을 선택합니다.
3. 목록에서 정책을 삽입할 사용자 또는 그룹 이름을 선택합니다.
4. 권한 탭을 선택하고 필요하다면 Permissions policies(권한 정책) 섹션을 확장합니다.
5. 권한 추가 및 인라인 정책 생성을 선택합니다.
6. 정책 생성 화면의 정책 편집기 섹션에서 JSON을 선택합니다.

   다음 JSON 명령문을 사용하여 정책 문서를 생성한 후 다음을 선택합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sso:GetManagedApplicationInstance",
        "sso:ListProfiles",
        "sso:GetProfiles",
        "sso:AssociateProfile",
        "sso:DisassociateProfile",
```

```
        "sso:GetProfile"
      ],
      "Resource": "*"
    }
  ]
}
```

7. 정책 검토 화면에서 정책 이름을 입력합니다. 정책에 만족하면 정책 생성을 선택합니다. 화면 상단에 있는 빨간색 상자에 표시되는 오류가 있지 않은지 확인합니다. 표시되는 오류가 있다면 수정합니다.

(선택 사항) IAM 보안 주체를 키 사용자로 추가하여 KMS (키 관리 서비스) 의 고객 관리 AWS 키로 Amazon DataZone 도메인을 생성합니다.

KMS (키 관리 서비스) 의 고객 관리 AWS 키 (CMK) 를 사용하여 Amazon DataZone 도메인을 선택적으로 생성하려면 먼저 다음 절차를 완료하여 IAM 보안 주체를 KMS 키 사용자로 설정하십시오.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/kms/ 에서 KMS 콘솔을 엽니다.
2. 해당 계정에서 직접 생성하고 관리하는 키를 보려면 탐색 창에서 고객 관리형 키를 선택합니다.
3. KMS 키 목록에서 검사하려는 KMS 키의 별칭 또는 키 ID를 선택합니다.
4. 주요 사용자를 추가 또는 제거하고 외부 AWS 계정의 KMS 키 사용을 허용하거나 허용하지 않으려면 페이지의 주요 사용자 섹션에 있는 컨트롤을 사용하십시오. 키 사용자는 암호화, 암호 해독, 재암호화 및 데이터 키 생성 같은 암호화 작업에서 KMS 키를 사용할 수 있습니다.

Amazon DataZone 데이터 포털을 사용하는 데 필요한 IAM 권한을 구성합니다.

Amazon DataZone 데이터 포털 또는 카탈로그를 사용하려는 모든 사용자, 그룹 또는 역할에는 필요한 권한이 있어야 합니다.

주제

- Amazon DataZone 데이터 포털 액세스에 필요한 정책을 사용자, 그룹 또는 역할에 연결
- Amazon DataZone 카탈로그 액세스에 필요한 정책을 사용자, 그룹 또는 역할에 연결
- KMS (Key Management Service) 의 고객 관리 키로 도메인을 암호화한 경우 Amazon DataZone 데이터 포털 또는 카탈로그 액세스에 대한 선택적 정책을 사용자, 그룹 또는 역할에 연결합니다. AWS

Amazon DataZone 데이터 포털 액세스에 필요한 정책을 사용자, 그룹 또는 역할에 연결

AWS 자격 증명 또는 싱글 사인온 (SSO) 자격 증명을 사용하여 Amazon DataZone 데이터 포털에 액세스할 수 있습니다. 아래 섹션의 지침에 따라 자격 증명으로 데이터 포털에 액세스하는 데 필요한 권한을 설정하십시오. AWS Amazon을 DataZone SSO와 함께 사용하는 방법에 대한 자세한 내용은 을 참조하십시오아마존용 AWS IAM 아이덴티티 센터 설정 DataZone.

> **Note**
>
> 도메인 AWS 계정의 IAM 보안 주체만 도메인의 데이터 포털에 액세스할 수 있습니다. 다른 AWS 계정의 IAM 보안 주체는 도메인의 데이터 포털에 액세스할 수 없습니다.

필요한 정책을 사용자, 그룹 또는 역할에 연결하려면 다음 절차를 완료하십시오. 자세한 정보는 AWS 아마존 관리형 정책 DataZone을 참조하세요.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/iam/ 에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 사용자, 사용자 그룹 또는 역할을 선택합니다.
3. 목록에서 정책을 내장할 사용자, 그룹 또는 역할의 이름을 선택합니다.
4. 권한 탭을 선택하고 필요하다면 Permissions policies(권한 정책) 섹션을 확장합니다.
5. 권한 추가 및 인라인 정책 생성 링크를 선택합니다.
6. 정책 생성 화면의 정책 편집기 섹션에서 JSON을 선택합니다. 다음 JSON 명령문을 사용하여 정책 문서를 생성한 후 다음을 선택합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "datazone:GetIamPortalLoginUrl"
            ],
            "Resource": [
                "*"
            ]
        }
```

```
    ]
}
```

7. 정책 검토 화면에서 정책 이름을 입력합니다. 정책에 만족하면 정책 생성을 선택합니다. 화면 상단에 있는 빨간색 상자에 표시되는 오류가 있지 않은지 확인합니다. 표시되는 오류가 있다면 수정합니다.

Amazon DataZone 카탈로그 액세스에 필요한 정책을 사용자, 그룹 또는 역할에 연결

> **Note**
>
> 도메인 AWS 계정의 IAM 보안 주체만 도메인 카탈로그에 액세스할 수 있습니다. 다른 AWS 계정의 IAM 보안 주체는 도메인의 카탈로그에 액세스할 수 없습니다.

다음 절차에 따라 API 및 SDK를 통해 Amazon DataZone 도메인 카탈로그에 대한 액세스 권한을 IAM ID에 부여할 수 있습니다. 이러한 IAM ID가 Amazon DataZone 데이터 포털에도 액세스할 수 있도록 하려면 위의 절차를 추가로 따르십시오. Amazon DataZone 데이터 포털 액세스에 필요한 정책을 사용자, 그룹 또는 역할에 연결 자세한 정보는 AWS 아마존 관리형 정책 DataZone을 참조하세요.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/iam/ 에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 정책을 선택합니다.
3. 정책 목록에서 정책 옆에 있는 라디오 버튼을 선택합니다. AmazonDataZoneFullUserAccess [Filter] 메뉴와 검색 상자를 사용하여 정책 목록을 필터링할 수 있습니다. 자세한 내용은 AWS 관리형 정책: AmazonDataZoneFullUserAccess단원을 참조하세요.
4. 작업(Actions)을 선택한 후 연결(Attach)을 선택합니다.
5. 각 보안 주체 옆의 확인란을 선택하여 정책을 연결할 사용자, 그룹 또는 역할을 선택합니다. 필터 메뉴와 검색 상자를 사용하면 보안 주체 개체 목록을 필터링할 수 있습니다. 사용자, 그룹 또는 역할을 선택한 후 Attach policy (정책 연결) 를 선택합니다.

KMS (Key Management Service) 의 고객 관리 키로 도메인을 암호화한 경우 Amazon DataZone 데이터 포털 또는 카탈로그 액세스에 대한 선택적 정책을 사용자, 그룹 또는 역할에 연결합니다. AWS

데이터 암호화를 위한 자체 KMS 키로 Amazon DataZone 도메인을 생성하는 경우, 다음 권한을 포함하는 인라인 정책을 생성하고 이를 IAM 보안 주체에 연결해야 Amazon DataZone 데이터 포털 또는 카탈로그에 액세스할 수 있습니다.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/iam/ 에서 IAM 콘솔을 엽니다.
2. 탐색 창에서 사용자, 사용자 그룹 또는 역할을 선택합니다.
3. 목록에서 정책을 내장할 사용자, 그룹 또는 역할의 이름을 선택합니다.
4. 권한 탭을 선택하고 필요하다면 Permissions policies(권한 정책) 섹션을 확장합니다.
5. 권한 추가 및 인라인 정책 생성 링크를 선택합니다.
6. 정책 생성 화면의 정책 편집기 섹션에서 JSON을 선택합니다. 다음 JSON 명령문을 사용하여 정책 문서를 생성한 후 다음을 선택합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        }
    ]
}
```

7. 정책 검토 화면에서 정책 이름을 입력합니다. 정책에 만족하면 정책 생성을 선택합니다. 화면 상단에 있는 빨간색 상자에 표시되는 오류가 있지 않은지 확인합니다. 표시되는 오류가 있다면 수정합니다.

아마존용 AWS IAM 아이덴티티 센터 설정 DataZone

> **Note**
>
> AWS Amazon DataZone 도메인과 동일한 AWS 지역에서 ID 센터를 활성화해야 합니다. 현재 AWS ID 센터는 단일 AWS 지역에서만 활성화할 수 있습니다.

싱글 사인온 (SSO) 자격 증명 또는 자격 증명을 사용하여 Amazon DataZone 데이터 포털에 액세스할 수 있습니다. AWS 이 섹션의 지침에 따라 DataZone Amazon용 AWS IAM ID 센터를 설정하십시오. AWS 자격 DataZone 증명으로 Amazon을 사용하는 방법에 대한 자세한 내용은 을 참조하십시오Amazon DataZone 관리 콘솔을 사용하는 데 필요한 IAM 권한을 구성합니다..

Amazon 도메인을 생성하려는 동일한 AWS 지역에서 이미 AWS IAM Identity Center (Single AWS Sign-On의 후속) 를 활성화하고 구성한 경우 이 섹션의 절차를 건너뛸 수 있습니다. DataZone

다음 절차를 완료하여 AWS IAM ID 센터 (싱글 사인온의 후속 센터) 를 활성화하십시오. AWS

1. AWS IAM ID 센터를 활성화하려면 AWS Organizations AWS 관리 계정의 자격 증명을 사용하여 관리 콘솔에 로그인해야 합니다. AWS Organizations 회원 계정의 자격 증명으로 로그인한 상태에서는 IAM Identity Center를 활성화할 수 없습니다. 자세한 내용은 Organizations 사용 안내서의 AWS 조직 만들기 및 관리를 참조하십시오.
2. AWS IAM ID 센터 (Single AWS Sign-On의 후속) 콘솔을 열고 상단 탐색 표시줄의 지역 선택기를 사용하여 Amazon 도메인을 생성할 AWS 지역을 선택합니다. DataZone
3. 활성화를 선택합니다.
4. 자격 증명 소스를 선택합니다.

   기본적으로 빠르고 쉬운 사용자 관리를 위한 IAM ID 센터 스토어가 제공됩니다. 선택적으로 외부 ID 공급자를 대신 연결할 수도 있습니다. 이 절차에서는 기본 IAM ID 센터 스토어를 사용합니다.

   자세한 내용은 ID 소스 선택을 참조하십시오.
5. IAM Identity Center 탐색 창에서 그룹을 선택하고 그룹 생성을 선택합니다. 그룹 이름을 입력하고 [Create] 를 선택합니다.
6. IAM ID 센터 탐색 창에서 [사용자] 를 선택합니다.
7. 사용자 추가 화면에서 필수 정보를 입력하고 사용자에게 암호 설정 지침이 포함된 이메일 보내기를 선택합니다. 사용자는 다음 설정 단계에 대한 이메일을 받게 됩니다.

8. 다음: 그룹을 선택하고 원하는 그룹을 선택한 다음 사용자 추가를 선택합니다. 사용자는 SSO를 사용하도록 초대하는 이메일을 받아야 합니다. 이 이메일에서 사용자는 초대 수락을 선택하고 비밀번호를 설정해야 합니다.

Amazon DataZone 도메인을 생성한 후 Amazon용 AWS ID 센터를 활성화하고 SSO 사용자 DataZone 및 SSO 그룹에 액세스 권한을 제공할 수 있습니다. 자세한 내용은 Amazon용 IAM 자격 증명 센터 활성화 DataZone을(를) 참조하세요.

시작하기

이 섹션의 정보는 Amazon 사용을 시작하는 데 도움이 DataZone 됩니다. DataZoneAmazon을 처음 사용하는 경우 에 제시된 개념과 용어에 익숙해지는 것부터 시작하십시오. 아마존 DataZone 용어 및 개념

이 시작하기 섹션에서는 다음과 같은 Amazon DataZone 퀵스타트 워크플로를 안내합니다.

주제

- AWS Glue 데이터를 사용한 Amazon DataZone 퀵스타트
- 아마존 DataZone Redshift 데이터를 활용한 아마존 퀵스타트
- 샘플 스크립트를 사용한 Amazon DataZone 퀵스타트

> **Important**
>
> 이러한 퀵스타트 워크플로의 단계를 시작하기 전에 이 안내서의 설정 섹션에 설명된 절차를 완료해야 합니다. 새 AWS 계정을 사용하는 경우 Amazon DataZone 관리 콘솔을 사용하는 데 필요한 권한을 구성해야 합니다. 기존 AWS Glue Data Catalog 객체가 있는 AWS 계정을 사용하는 경우 Amazon에 대한 Lake Formation 권한도 구성해야 DataZone 합니다.

AWS Glue 데이터를 사용한 Amazon DataZone 퀵스타트

주제

- 1단계 - Amazon DataZone 도메인 및 데이터 포털 생성
- 2단계 - 퍼블리싱 프로젝트 만들기
- 3단계 - 환경 만들기
- 4단계 - 게시용 데이터 생성
- 5단계 - AWS Glue에서 메타데이터 수집
- 6단계 - 데이터 자산을 큐레이션하고 게시합니다.
- 7단계 - 데이터 분석을 위한 프로젝트 만들기
- 8단계 - 데이터 분석을 위한 환경 만들기
- 9단계 - 데이터 카탈로그 검색 및 데이터 구독

- 10단계 - 구독 요청 승인
- 11단계 - Amazon Athena에서 쿼리 작성 및 데이터 분석

1단계 - Amazon DataZone 도메인 및 데이터 포털 생성

이 섹션에서는 이 워크플로를 위한 Amazon DataZone 도메인 및 데이터 포털을 생성하는 단계를 설명합니다.

Amazon DataZone 도메인을 생성하려면 다음 절차를 완료하십시오. Amazon DataZone 도메인에 대한 자세한 내용은 을 참조하십시오아마존 DataZone 용어 및 개념.

1. https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 로그인한 다음 도메인 생성을 선택합니다.

   > **Note**
   >
   > 이 워크플로에 기존 Amazon DataZone 도메인을 사용하려면 도메인 보기를 선택한 다음 사용할 도메인을 선택한 다음 게시 프로젝트 생성의 2단계로 진행하십시오.

2. 도메인 생성 페이지에서 다음 필드에 값을 입력합니다.

   - 이름 - 도메인의 이름을 지정합니다. 이 워크플로의 목적상 이 도메인을 마케팅이라고 부를 수 있습니다.
   - 설명 - 선택적 도메인 설명을 지정합니다.
   - 데이터 암호화 - 사용자 대신 AWS 소유하고 관리하는 키로 데이터가 기본적으로 암호화됩니다. 이 사용 사례에서는 기본 데이터 암호화 설정을 그대로 둘 수 있습니다.

     고객 관리 키 사용에 대한 자세한 내용은 을 참조하십시오Amazon의 유휴 데이터 암호화 DataZone. 데이터 암호화에 자체 KMS 키를 사용하는 경우 AmazonDataZoneDomainExecutionRole 기본값에 다음 설명을 포함해야 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
```

```
        "kms:GenerateDataKey"
      ],
      "Resource": "*"
    }
  ]
}
```

- 서비스 액세스 - 기본적으로 선택된 상태로 둡니다. 기본 역할 사용 옵션은 변경하지 마십시오.

> **Note**
>
> 이 워크플로에 기존 Amazon DataZone 도메인을 사용하는 경우 기존 서비스 역할 사용 옵션을 선택한 다음 드롭다운 메뉴에서 기존 역할을 선택할 수 있습니다.

- 빠른 설정에서 데이터 사용 및 게시를 위해 이 계정 설정을 선택합니다. 이 옵션은 데이터 레이크 및 데이터 웨어하우스의 내장된 Amazon DataZone 청사진을 활성화하고 이 계정에 필요한 권한, 리소스, 기본 프로젝트, 기본 데이터 레이크 및 데이터 웨어하우스 환경 프로필을 구성합니다. Amazon DataZone 블루프린트에 대한 자세한 내용은 을 참조하십시오아마존 DataZone 용어 및 개념.
- 권한 세부 정보 아래의 나머지 필드는 변경하지 마십시오.

> **Note**
>
> 기존 Amazon DataZone 도메인이 있는 경우 기존 서비스 역할 사용 옵션을 선택한 다음 드롭다운 메뉴에서 Glue 관리 액세스 역할, Redshift 액세스 관리 역할 및 프로비저닝 역할에 대한 기존 역할을 선택할 수 있습니다.

- 태그 아래의 필드를 변경하지 않고 그대로 두십시오.
- 도메인 생성(Create domain)을 선택합니다.

3. 도메인이 성공적으로 생성되면 이 도메인을 선택하고 도메인의 요약 페이지에서 이 도메인의 데이터 포털 URL을 기록해 둡니다. 이 URL을 사용하여 Amazon DataZone 데이터 포털에 액세스하여 이 워크플로의 나머지 단계를 완료할 수 있습니다. 오픈 데이터 포털을 선택하여 데이터 포털로 이동할 수도 있습니다.

> **Note**
>
> DataZoneAmazon의 현재 릴리스에서는 도메인이 생성된 후에는 데이터 포털용으로 생성된 URL을 수정할 수 없습니다.

도메인 생성을 완료하는 데 몇 분이 걸릴 수 있습니다. 다음 단계로 진행하기 전에 도메인이 사용 가능 상태가 될 때까지 기다리십시오.

2단계 - 퍼블리싱 프로젝트 만들기

이 섹션에서는 이 워크플로의 퍼블리싱 프로젝트를 만드는 데 필요한 단계를 설명합니다.

1. 위의 1단계를 완료하고 도메인을 생성하면 Amazon에 오신 것을 환영합니다 DataZone! 라는 메시지가 표시됩니다. 창. 이 창에서 프로젝트 생성을 선택합니다.
2. 프로젝트 이름을 지정합니다. 예를 들어 이 워크플로의 경우 이름을 지정하고 나머지 필드는 변경하지 않고 만들기를 선택할 수 있습니다. SalesDataPublishingProject

3단계 - 환경 만들기

이 섹션에서는 이 워크플로를 위한 환경을 만드는 데 필요한 단계를 설명합니다.

1. 위의 2단계를 완료하고 프로젝트를 만들면 프로젝트 준비 완료 창이 나타납니다. 이 창에서 환경 만들기를 선택합니다.
2. 환경 만들기 페이지에서 다음을 지정한 다음 환경 만들기를 선택합니다.
3. 다음에 대한 값을 지정합니다.
   - 이름 - 환경 이름을 지정합니다. 이 안내에서는 이름을 호출할 수 있습니다. `Default data lake environment`
   - 설명 - 환경에 대한 설명을 지정합니다.
   - 환경 프로필 - DataLakeProfile환경 프로필을 선택합니다. 이렇게 하면 이 DataZone 워크플로에서 Amazon을 사용하여 Amazon S3, AWS Glue 카탈로그 및 Amazon Athena의 데이터로 작업할 수 있습니다.
   - 이 연습에서는 나머지 필드는 변경하지 않고 그대로 두십시오.
4. 환경 생성을 선택합니다.

4단계 - 게시용 데이터 생성

이 섹션에서는 이 워크플로우에서 게시할 데이터를 생성하는 데 필요한 단계를 설명합니다.

1. 위의 3단계를 완료하면 SalesDataPublishingProject 프로젝트의 오른쪽 패널에 있는 분석 도구 아래에서 Amazon Athena를 선택합니다. 그러면 프로젝트 자격 증명을 인증에 사용하는 Athena 쿼리 편집기가 열립니다. Amazon DataZone 환경 드롭다운에서 게시 환경을 선택하고 <environment_name>%_pub_db 데이터베이스가 쿼리 편집기에서처럼 선택되었는지 확인하십시오.
2. 이 안내에서는 Create as Select (Create as Select) 쿼리 스크립트를 사용하여 Amazon에 게시할 새 테이블을 생성합니다. DataZone 쿼리 편집기에서 이 CTAS 스크립트를 실행하여 게시하고 검색 및 구독에 사용할 수 있는 mkt_sls_table 테이블을 생성합니다.

```
CREATE TABLE mkt_sls_table AS
SELECT 146776932 AS ord_num, 23 AS sales_qty_sld, 23.4 AS wholesale_cost, 45.0 as
 lst_pr, 43.0 as sell_pr, 2.0 as disnt, 12 as ship_mode,13 as warehouse_id, 23 as
 item_id, 34 as ctlg_page, 232 as ship_cust_id, 4556 as bill_cust_id
UNION ALL SELECT 46776931, 24, 24.4, 46, 44, 1, 14, 15, 24, 35, 222, 4551
UNION ALL SELECT 46777394, 42, 43.4, 60, 50, 10, 30, 20, 27, 43, 241, 4565
UNION ALL SELECT 46777831, 33, 40.4, 51, 46, 15, 16, 26, 33, 40, 234, 4563
UNION ALL SELECT 46779160, 29, 26.4, 50, 61, 8, 31, 15, 36, 40, 242, 4562
UNION ALL SELECT 46778595, 43, 28.4, 49, 47, 7, 28, 22, 27, 43, 224, 4555
UNION ALL SELECT 46779482, 34, 33.4, 64, 44, 10, 17, 27, 43, 52, 222, 4556
UNION ALL SELECT 46779650, 39, 37.4, 51, 62, 13, 31, 25, 31, 52, 224, 4551
UNION ALL SELECT 46780524, 33, 40.4, 60, 53, 18, 32, 31, 31, 39, 232, 4563
UNION ALL SELECT 46780634, 39, 35.4, 46, 44, 16, 33, 19, 31, 52, 242, 4557
UNION ALL SELECT 46781887, 24, 30.4, 54, 62, 13, 18, 29, 24, 52, 223, 4561
```

   왼쪽의 테이블 및 뷰 섹션에서 mkt_sls_table 테이블이 성공적으로 생성되었는지 확인하십시오. 이제 Amazon DataZone 카탈로그에 게시할 수 있는 데이터 자산이 생겼습니다.

5단계 - AWS Glue에서 메타데이터 수집

이 섹션에서는 이 워크플로를 위해 AWS Glue에서 메타데이터를 수집하는 단계를 설명합니다.

1. 위의 4단계를 완료하면 Amazon DataZone 데이터 포털에서 SalesDataPublishingProject 프로젝트를 선택하고 데이터 탭을 선택한 다음 왼쪽 패널에서 데이터 소스를 선택합니다.

2. 환경 생성 프로세스의 일부로 생성된 소스를 선택합니다.
3. 작업 드롭다운 메뉴 옆의 실행을 선택한 다음 새로 고침 버튼을 선택합니다. 데이터 소스 실행이 완료되면 자산이 Amazon DataZone 인벤토리에 추가됩니다.

6단계 - 데이터 자산을 큐레이션하고 게시합니다.

이 섹션에서는 이 워크플로우에서 데이터 자산을 큐레이션하고 게시하는 단계를 설명합니다.

1. 위의 5단계를 완료하면 Amazon DataZone 데이터 포털에서 이전 단계에서 생성한 `SalesDataPublishingProject` 프로젝트를 선택하고 데이터 탭을 선택한 다음 왼쪽 패널에서 인벤토리 데이터를 선택하고 `mkt_sls_table` 테이블을 찾습니다.
2. `mkt_sls_table`자산의 세부 정보 페이지를 열어 자동으로 생성된 비즈니스 이름을 확인하십시오. 자산 및 열에 대해 자동 생성된 이름을 보려면 자동 생성된 메타데이터 아이콘을 선택합니다. 각 이름을 개별적으로 허용 또는 거부하거나 모두 수락을 선택하여 생성된 이름을 적용할 수 있습니다. 선택적으로 사용 가능한 메타데이터 양식을 자산에 추가하고 용어집 용어를 선택하여 데이터를 분류할 수도 있습니다.
3. 에셋 게시를 선택하여 에셋을 게시합니다. `mkt_sls_table`

7단계 - 데이터 분석을 위한 프로젝트 만들기

이 섹션에서는 데이터 분석을 위한 프로젝트를 만드는 단계를 설명합니다. 이것이 이 워크플로의 데이터 소비자 단계의 시작입니다.

1. 위의 6단계를 완료한 후 Amazon DataZone 데이터 포털의 프로젝트 드롭다운 메뉴에서 Create project 를 선택합니다.
2. Create project 페이지에서 프로젝트 이름을 지정합니다. 예를 들어 이 워크플로의 경우 이름을 지정하고 나머지 필드는 변경하지 않고 그대로 둔 다음 Create를 선택할 수 있습니다. MarketingDataAnalysisProject

8단계 - 데이터 분석을 위한 환경 만들기

이 섹션에서는 데이터 분석을 위한 환경을 만드는 단계를 설명합니다.

1. 위의 7단계를 완료하면 Amazon DataZone 데이터 포털에서 `MarketingDataAnalysisProject` 프로젝트를 선택한 다음 환경 탭을 선택한 다음 환경 생성을 선택합니다.

2. 환경 생성 페이지에서 다음을 지정한 다음 환경 생성을 선택합니다.

   - 이름 - 환경 이름을 지정합니다. 이 안내에서는 이름을 호출할 수 있습니다. `Default data lake environment`
   - 설명 - 환경에 대한 설명을 지정합니다.
   - 환경 프로필 - 기본 제공 DataLakeProfile환경 프로필을 선택합니다.
   - 이 연습에서는 나머지 필드는 변경하지 마십시오.

9단계 - 데이터 카탈로그 검색 및 데이터 구독

이 섹션에서는 데이터 카탈로그를 검색하고 데이터를 구독하는 단계를 설명합니다.

1. 위의 8단계를 완료하면 Amazon DataZone 데이터 포털에서 Amazon DataZone 아이콘을 선택하고 Amazon DataZone Search 필드에서 데이터 포털의 검색 표시줄에 있는 키워드 (예: '카탈로그' 또는 '판매') 를 사용하여 데이터 자산을 검색합니다.

   필요한 경우 필터 또는 정렬을 적용하고 제품 판매 데이터 자산을 찾으면 해당 자산을 선택하여 자산의 세부 정보 페이지를 열 수 있습니다.
2. 카탈로그 판매 데이터 자산의 세부 정보 페이지에서 구독을 선택합니다.
3. 구독 대화 상자의 드롭다운에서 MarketingDataAnalysisProject소비자 프로젝트를 선택한 다음 구독 요청 이유를 지정하고 구독을 선택합니다.

10단계 - 구독 요청 승인

이 섹션에서는 구독 요청을 승인하는 단계를 설명합니다.

1. 위의 9단계를 완료한 후 Amazon DataZone 데이터 포털에서 자산을 게시하는 데 사용한 SalesDataPublishingProject프로젝트를 선택합니다.
2. 데이터 탭을 선택한 다음 게시된 데이터를 선택한 다음 수신 요청을 선택합니다.
3. 이제 승인이 필요한 새 요청의 행을 볼 수 있습니다. 요청 보기를 선택합니다. 승인 이유를 입력하고 승인을 선택합니다.

11단계 - Amazon Athena에서 쿼리 작성 및 데이터 분석

Amazon DataZone 카탈로그에 자산을 성공적으로 게시하고 구독했으므로 이제 자산을 분석할 수 있습니다.

1. Amazon DataZone 데이터 포털에서 MarketingDataAnalysisProject소비자 프로젝트를 선택한 다음 오른쪽 패널의 분석 도구에서 Amazon Athena를 사용한 쿼리 데이터 링크를 선택합니다. 그러면 인증을 위해 프로젝트의 자격 증명을 사용하는 Amazon Athena 쿼리 편집기가 열립니다. 쿼리 편집기의 Amazon DataZone Environment 드롭다운에서 MarketingDataAnalysisProject소비자 환경을 선택한 다음 데이터베이스 `<environment_name>%sub_db` 드롭다운에서 프로젝트를 선택합니다.
2. 이제 구독한 테이블에서 쿼리를 실행할 수 있습니다. 테이블 및 뷰에서 테이블을 선택한 다음 [미리 보기] 를 선택하여 편집기 화면에 select 명령문을 표시할 수 있습니다. 쿼리를 실행하여 결과를 확인합니다.

아마존 DataZone Redshift 데이터를 활용한 아마존 퀵스타트

주제

1단계 - Amazon DataZone 도메인 및 데이터 포털 생성

Amazon DataZone 도메인을 생성하려면 다음 절차를 완료하십시오. Amazon DataZone 도메인에 대한 자세한 내용은 을 참조하십시오아마존 DataZone 용어 및 개념.

1. https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 로그인한 다음 도메인 생성을 선택합니다.

> **Note**
>
> 이 워크플로에 기존 Amazon DataZone 도메인을 사용하려면 도메인 보기를 선택한 다음 사용할 도메인을 선택한 다음 게시 프로젝트 생성의 2단계로 진행하십시오.

2. 도메인 생성 페이지에서 다음 필드에 값을 입력합니다.

- 이름 - 도메인의 이름을 지정합니다. 이 워크플로의 목적에 따라 이 도메인을 호출할 수 `Marketing` 있습니다.
- 설명 - 선택적 도메인 설명을 지정합니다.
- 데이터 암호화 - 사용자 대신 AWS 소유하고 관리하는 키로 데이터가 기본적으로 암호화됩니다. 이 안내에서는 기본 데이터 암호화 설정을 그대로 둘 수 있습니다.

  고객 관리 키 사용에 대한 자세한 내용은 을 참조하십시오. Amazon의 유휴 데이터 암호화 DataZone 데이터 암호화에 자체 KMS 키를 사용하는 경우 AmazonDataZoneDomainExecutionRole 기본값에 다음 설명을 포함해야 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "*"
    }
  ]
}
```

- 서비스 액세스 - 사용자 지정 서비스 역할 사용 옵션을 선택한 다음 AmazonDataZoneDomainExecutionRole드롭다운 메뉴에서 선택합니다.
- 빠른 설정에서 이 계정을 데이터 사용 및 게시용으로 설정을 선택합니다. 이 옵션은 데이터 레이크 및 데이터 웨어하우스의 내장된 Amazon DataZone 블루프린트를 활성화하고 이 워크플로의 나머지 단계를 완료하는 데 필요한 권한과 리소스를 구성합니다. Amazon DataZone 블루프린트에 대한 자세한 내용은 을 참조하십시오아마존 DataZone 용어 및 개념.

- 권한 세부 정보 및 태그 아래의 나머지 필드를 변경하지 않고 유지한 다음 Create domain (도메인 생성) 을 선택합니다.

3. 도메인이 성공적으로 생성되면 이 도메인을 선택하고 도메인의 요약 페이지에서 이 도메인의 데이터 포털 URL을 기록해 둡니다. 이 URL을 사용하여 Amazon DataZone 데이터 포털에 액세스하여 이 워크플로의 나머지 단계를 완료할 수 있습니다.

> **Note**
>
> DataZoneAmazon의 현재 릴리스에서는 도메인이 생성된 후에는 데이터 포털용으로 생성된 URL을 수정할 수 없습니다.

도메인 생성을 완료하는 데 몇 분이 걸릴 수 있습니다. 다음 단계로 진행하기 전에 도메인이 사용 가능 상태가 될 때까지 기다리십시오.

2단계 - 퍼블리싱 프로젝트 만들기

다음 섹션에서는 이 워크플로우에서 게시 프로젝트를 만드는 단계를 설명합니다.

1. 1단계를 완료하면 데이터 포털 URL을 사용하여 Amazon DataZone 데이터 포털로 이동하고 싱글 사인온 (SSO) 또는 AWS IAM 자격 증명을 사용하여 로그인합니다.
2. Create project (프로젝트 생성) 를 선택하고 프로젝트 이름을 지정합니다. 예를 들어 이 워크플로의 경우 이름을 지정하고 나머지 필드는 변경하지 않고 그대로 둔 다음 [Create] 를 선택합니다. SalesDataPublishingProject

3단계 - 환경 만들기

다음 섹션에서는 이 워크플로우에서 환경을 만드는 단계를 설명합니다.

1. 2단계를 완료하면 Amazon DataZone 데이터 포털에서 이전 단계에서 생성한 `SalesDataPublishingProject` 프로젝트를 선택한 다음 환경 탭을 선택한 다음 환경 생성을 선택합니다.
2. 환경 생성 페이지에서 다음을 지정한 다음 환경 생성을 선택합니다.

   - 이름 - 환경 이름을 지정합니다. 이 안내에서는 이름을 호출할 수 있습니다. `Default data warehouse environment`
   - 설명 - 환경에 대한 설명을 지정합니다.

- 환경 프로필 - DataWarehouseProfile환경 프로필을 선택합니다.
- Amazon Redshift 클러스터의 이름, 데이터베이스 이름, 그리고 데이터가 저장되어 있는 Amazon Redshift 클러스터의 보안 ARN을 제공하십시오.

> **Note**
>
> AWS Secrets Manager의 시크릿에 다음 태그 (키/값) 가 포함되어 있는지 확인하세요.
>
> - Amazon Redshift 클러스터의 경우 - 데이터 존.rs.cluster: <cluster_name:database name>
>
> Amazon Redshift 서버리스 워크그룹의 경우 - 데이터존.rs.워크그룹: <workgroup_name:database_name>
> - AmazonDataZoneProject: <projectID>
> - AmazonDataZoneDomain: <domainID>
>
> 자세한 내용은 AWS Secrets Manager에 데이터베이스 자격 증명 저장을 참조하십시오. AWS Secrets Manager에서 제공하는 데이터베이스 사용자에게는 수퍼유저 권한이 있어야 합니다.

4단계 - 게시를 위한 데이터 생성

다음 섹션에서는 이 워크플로우에서 게시할 데이터를 생성하는 단계를 설명합니다.

1. 3단계를 완료하면 Amazon DataZone 데이터 포털에서 `SalesDataPublishingProject` 프로젝트를 선택한 다음 오른쪽 패널의 분석 도구에서 Amazon Redshift를 선택합니다. 그러면 인증을 위해 프로젝트의 자격 증명을 사용하는 Amazon Redshift 쿼리 편집기가 열립니다.
2. 이 안내에서는 Create as Select (Create as Select) 쿼리 스크립트를 사용하여 Amazon에 게시할 새 테이블을 생성합니다. DataZone 쿼리 편집기에서 이 CTAS 스크립트를 실행하여 게시하고 검색 및 구독에 사용할 수 있는 `mkt_sls_table` 테이블을 생성합니다.

```
CREATE TABLE mkt_sls_table AS
SELECT 146776932 AS ord_num, 23 AS sales_qty_sld, 23.4 AS wholesale_cost, 45.0 as
 lst_pr, 43.0 as sell_pr, 2.0 as disnt, 12 as ship_mode,13 as warehouse_id, 23 as
 item_id, 34 as ctlg_page, 232 as ship_cust_id, 4556 as bill_cust_id
UNION ALL SELECT 46776931, 24, 24.4, 46, 44, 1, 14, 15, 24, 35, 222, 4551
UNION ALL SELECT 46777394, 42, 43.4, 60, 50, 10, 30, 20, 27, 43, 241, 4565
UNION ALL SELECT 46777831, 33, 40.4, 51, 46, 15, 16, 26, 33, 40, 234, 4563
```

```
UNION ALL SELECT 46779160, 29, 26.4, 50, 61, 8, 31, 15, 36, 40, 242, 4562
UNION ALL SELECT 46778595, 43, 28.4, 49, 47, 7, 28, 22, 27, 43, 224, 4555
UNION ALL SELECT 46779482, 34, 33.4, 64, 44, 10, 17, 27, 43, 52, 222, 4556
UNION ALL SELECT 46779650, 39, 37.4, 51, 62, 13, 31, 25, 31, 52, 224, 4551
UNION ALL SELECT 46780524, 33, 40.4, 60, 53, 18, 32, 31, 31, 39, 232, 4563
UNION ALL SELECT 46780634, 39, 35.4, 46, 44, 16, 33, 19, 31, 52, 242, 4557
UNION ALL SELECT 46781887, 24, 30.4, 54, 62, 13, 18, 29, 24, 52, 223, 4561
```

mkt_sls_table 테이블이 성공적으로 생성되었는지 확인하십시오. 이제 Amazon DataZone 카탈로그에 게시할 수 있는 데이터 자산이 생겼습니다.

5단계 - 아마존 Redshift에서 메타데이터 수집

다음 섹션에서는 Amazon Redshift에서 메타데이터를 수집하는 단계를 설명합니다.

1. 4단계를 완료하면 Amazon DataZone 데이터 포털에서 `SalesDataPublishingProject` 프로젝트를 선택하고 데이터 탭을 선택한 다음 데이터 소스를 선택합니다.
2. 환경 생성 프로세스의 일부로 생성된 소스를 선택합니다.
3. 작업 드롭다운 메뉴 옆의 실행을 선택한 다음 새로 고침 버튼을 선택합니다. 데이터 소스 실행이 완료되면 자산이 Amazon DataZone 인벤토리에 추가됩니다.

6단계 - 데이터 자산을 큐레이션하고 게시합니다.

다음 섹션에서는 이 워크플로우에서 데이터 자산을 큐레이션하고 게시하는 단계를 설명합니다.

1. 5단계를 완료하면 Amazon DataZone 데이터 포털에서 `SalesDataPublishingProject` 프로젝트를 선택한 다음 데이터 탭을 선택하고 인벤토리 데이터를 선택한 다음 `mkt_sls_table` 테이블을 찾습니다.
2. `mkt_sls_table`자산의 세부 정보 페이지를 열어 자동으로 생성된 비즈니스 이름을 확인하십시오. 자산 및 열에 대해 자동 생성된 이름을 보려면 자동 생성된 메타데이터 아이콘을 선택합니다. 각 이름을 개별적으로 허용 또는 거부하거나 모두 수락을 선택하여 생성된 이름을 적용할 수 있습니다. 선택적으로 사용 가능한 메타데이터 양식을 자산에 추가하고 용어집 용어를 선택하여 데이터를 분류할 수도 있습니다.
3. [Publish] 를 선택하여 자산을 게시합니다. `mkt_sls_table`

7단계 - 데이터 분석을 위한 프로젝트 만들기

다음 섹션에서는 이 워크플로우에서 데이터 분석을 위한 프로젝트를 만드는 단계를 설명합니다.

1. 6단계를 완료한 후 Amazon DataZone 데이터 포털에서 프로젝트 생성을 선택합니다.
2. 프로젝트 생성 페이지에서 프로젝트 이름을 지정합니다. 예를 들어 이 워크플로의 경우 이름을 지정하고 나머지 필드는 변경하지 않고 그대로 둔 다음 Create를 선택할 수 있습니다. MarketingDataAnalysisProject

8단계 - 데이터 분석을 위한 환경 만들기

다음 섹션에서는 이 워크플로우에서 데이터 분석을 위한 환경을 만드는 단계를 설명합니다.

1. 7단계를 완료하면 Amazon DataZone 데이터 포털에서 이전 단계에서 생성한 `MarketingDataAnalysisProject` 프로젝트를 선택한 다음 환경 탭을 선택한 다음 Add environment (환경 추가) 를 선택합니다.
2. 환경 생성 페이지에서 다음을 지정한 다음 환경 생성을 선택합니다.
   - 이름 - 환경 이름을 지정합니다. 이 안내에서는 이름을 호출할 수 있습니다. `Default data warehouse environment`
   - 설명 - 환경에 대한 설명을 지정합니다.
   - 환경 프로필 - DataWarehouseProfile환경 프로필을 선택합니다.
   - Amazon Redshift 클러스터의 이름, 데이터베이스 이름, 그리고 데이터가 저장되어 있는 Amazon Redshift 클러스터의 보안 ARN을 제공하십시오.

> **Note**
>
> AWS Secrets Manager의 시크릿에 다음 태그 (키/값) 가 포함되어 있는지 확인하세요.
>
> - Amazon Redshift 클러스터의 경우 - 데이터 존.rs.cluster: <cluster_name:database name>
>
> Amazon Redshift 서버리스 워크그룹의 경우 - 데이터존.rs.워크그룹: <workgroup_name:database_name>
> - AmazonDataZoneProject: <projectID>
> - AmazonDataZoneDomain: <domainID>
>
> 자세한 내용은 AWS Secrets Manager에 데이터베이스 자격 증명 저장을 참조하십시오.

AWS Secrets Manager에서 제공하는 데이터베이스 사용자에게는 수퍼유저 권한이 있어야 합니다.

- 이 연습에서는 나머지 필드는 변경하지 않고 그대로 유지하세요.

9단계 - 데이터 카탈로그 검색 및 데이터 구독

다음 섹션에서는 데이터 카탈로그를 검색하고 데이터를 구독하는 단계를 설명합니다.

1. 8단계를 완료하면 Amazon DataZone 데이터 포털에서 데이터 포털의 검색 창에 있는 키워드 (예: '카탈로그' 또는 '판매') 를 사용하여 데이터 자산을 검색합니다.

   필요한 경우 필터 또는 정렬을 적용하고 제품 판매 데이터 자산을 찾으면 자산을 선택하여 자산의 세부 정보 페이지를 열 수 있습니다.
2. 제품 판매 데이터 자산의 세부 정보 페이지에서 구독을 선택합니다.
3. 대화 상자의 드롭다운에서 소비자 프로젝트를 선택하고 액세스 요청 이유를 입력한 다음 구독을 선택합니다.

10단계 - 구독 요청 승인

다음 섹션에서는 이 워크플로의 구독 요청을 승인하는 단계를 설명합니다.

1. 9단계를 완료하면 Amazon DataZone 데이터 포털에서 자산을 게시하는 데 사용한 SalesDataPublishingProject프로젝트를 선택합니다.
2. 데이터 탭, 게시된 데이터, 수신 요청을 차례로 선택합니다.
3. 요청 보기 링크를 선택한 다음 승인을 선택합니다.

11단계 - Amazon Redshift에서 쿼리 작성 및 데이터 분석

Amazon DataZone 카탈로그에 자산을 성공적으로 게시하고 구독했으므로 이제 자산을 분석할 수 있습니다.

1. 아마존 DataZone 데이터 포털의 오른쪽 패널에서 Amazon Redshift 링크를 클릭합니다. 그러면 인증을 위해 프로젝트 자격 증명을 사용하는 Amazon Redshift 쿼리 편집기가 열립니다.

2. 이제 구독 테이블에서 쿼리 (select 명령문) 를 실행할 수 있습니다. 테이블 (three-vertical-dots 옵션) 을 클릭하고 미리보기를 선택하여 편집기 화면에서 선택 명령문을 표시할 수 있습니다. 쿼리를 실행하여 결과를 확인합니다.

샘플 스크립트를 사용한 Amazon DataZone 퀵스타트

다음 섹션에서는 다음 작업을 완료하는 데 사용할 수 있는 다양한 Amazon DataZone API를 호출하는 샘플 스크립트를 설명합니다.

주제

- Amazon DataZone 도메인 및 데이터 포털 생성
- 퍼블리싱 프로젝트 생성
- 환경 프로필 생성
- 환경 생성
- AWS Glue에서 메타데이터 수집
- 데이터 자산 큐레이션 및 게시
- 데이터 카탈로그 검색 및 데이터 구독
- 기타 유용한 샘플 스크립트

Amazon DataZone 도메인 및 데이터 포털 생성

다음 샘플 스크립트를 사용하여 Amazon DataZone 도메인을 생성할 수 있습니다. Amazon DataZone 도메인에 대한 자세한 내용은 을 참조하십시오아마존 DataZone 용어 및 개념.

```
import sys
import boto3

// Initialize datazone client
region = 'us-east-1'
dzclient = boto3.client(service_name='datazone', region_name='us-east-1')

// Create DataZone domain
def create_domain(name):
    return dzclient.create_domain(
        name = name,
        description = "this is a description",
```

```
        domainExecutionRole = "arn:aws:iam::<account>:role/
AmazonDataZoneDomainExecutionRole",
    )
```

퍼블리싱 프로젝트 생성

다음 샘플 스크립트를 사용하여 Amazon에서 게시 프로젝트를 생성할 수 DataZone 있습니다.

```
// Create Project
def create_project(domainId):
    return dzclient.create_project(
        domainIdentifier = domainId,
        name = "sample-project"
    )
```

환경 프로필 생성

다음 샘플 스크립트를 사용하여 Amazon에서 환경 프로필을 생성할 수 DataZone 있습니다.

이 샘플 페이로드는 `CreateEnvironmentProfile` API가 호출될 때 사용됩니다.

```
Sample Payload
{
    "Content":{
        "project_name": "Admin_project",
        "domain_name": "Drug-Research-and-Development",
        "blueprint_account_region": [
            {
                "blueprint_name": "DefaultDataLake",
                "account_id": ["066535990535",
                "413878397724",
                "676266385322",
                "747721550195",
                "755347404384"
                ],
                "region": ["us-west-2", "us-east-1"]
            },
            {
                "blueprint_name": "DefaultDataWarehouse",
```

```
                "account_id": ["066535990535",
                "413878397724",
                "676266385322",
                "747721550195",
                "755347404384"
                ],
                "region":["us-west-2", "us-east-1"]
            }
        ]
    }
}
```

이 샘플 스크립트는 API를 호출합니다. CreateEnvironmentProfile

```
def create_environment_profile(domain_id, project_id, env_blueprints)
        try:
            response = dz.list_environment_blueprints(
                domainIdentifier=domain_id,
                managed=True
            )
            env_blueprints = response.get("items")
            env_blueprints_map = {}
            for i in env_blueprints:
                env_blueprints_map[i["name"]] = i['id']

            print("Environment Blueprint map", env_blueprints_map)
            for i in blueprint_account_region:
                print(i)
                for j in i["account_id"]:
                    for k in i["region"]:
                        print("The env blueprint name is", i['blueprint_name'])
                        dz.create_environment_profile(
                            description='This is a test environment profile created via
 lambda function',
                            domainIdentifier=domain_id,
                            awsAccountId=j,
                            awsAccountRegion=k,

 environmentBlueprintIdentifier=env_blueprints_map.get(i["blueprint_name"]),
                            name=i["blueprint_name"] + j + k + "_profile",
                            projectIdentifier=project_id
```

```
                        )
        except Exception as e:
            print("Failed to created Environment Profile")
            raise e
```

다음은 CreateEnvironmentProfile API가 호출된 후의 샘플 출력 페이로드입니다.

```
{
    "Content":{
        "project_name": "Admin_project",
        "domain_name": "Drug-Research-and-Development",
        "blueprint_account_region": [
            {
                "blueprint_name": "DefaultDataWarehouse",
                "account_id": ["111111111111"],
                "region":["us-west-2"],
                "user_parameters":[
                    {
                        "name": "dataAccessSecretsArn",
                        "value": ""
                    }
                ]
            }
        ]
    }
}
```

환경 생성

다음 샘플 스크립트를 사용하여 Amazon에서 환경을 생성할 수 DataZone 있습니다.

```
def create_environment(domain_id, project_id,blueprint_account_region ):
         try:
            #refer to get_domain_id and get_project_id for fetching ids using names.
            sts_client = boto3.client("sts")
            # Get the current account ID
            account_id = sts_client.get_caller_identity()["Account"]
            print("Fetching environment profile ids")
            env_profile_map = get_env_profile_map(domain_id, project_id)
```

```
            for i in blueprint_account_region:
                for j in i["account_id"]:
                    for k in i["region"]:
                        print(" env blueprint name", i['blueprint_name'])
                        profile_name = i["blueprint_name"] + j + k + "_profile"
                        env_name = i["blueprint_name"] + j + k + "_env"
                        description = f'This is environment is created for
{profile_name}, Account {account_id} and region {i["region"]}'
                        try:
                            dz.create_environment(
                                description=description,
                                domainIdentifier=domain_id,

environmentProfileIdentifier=env_profile_map.get(profile_name),
                                name=env_name,
                                projectIdentifier=project_id
                            )
                            print(f"Environment created - {env_name}")
                        except:
                            dz.create_environment(
                                description=description,
                                domainIdentifier=domain_id,

environmentProfileIdentifier=env_profile_map.get(profile_name),
                                name=env_name,
                                projectIdentifier=project_id,
                                userParameters= i["user_parameters"]
                            )
                            print(f"Environment created - {env_name}")
        except Exception as e:
            print("Failed to created Environment")
            raise e
```

AWS Glue에서 메타데이터 수집

이 샘플 스크립트를 사용하여 AWS Glue에서 메타데이터를 수집할 수 있습니다. 이 스크립트는 표준 일정에 따라 실행됩니다. 샘플 스크립트에서 매개 변수를 검색하여 전역으로 만들 수 있습니다. 표준 함수를 사용하여 프로젝트, 환경 및 도메인 ID를 가져옵니다. AWS Glue 데이터 소스는 표준 시간에 생성되고 실행되며 스크립트의 cron 섹션에서 업데이트할 수 있습니다.

```
def crcreate_data_source(domain_id, project_id,data_source_name)
        print("Creating Data Source")
        data_source_creation = dz.create_data_source(
            # Define data source : Customize the data source to which you'd like to
 connect
            # define the name of the Data source to create, example: name
 ='TestGlueDataSource'
            name=data_source_name,
            # give a description for the datasource (optional), example:
 description='This is a dorra test for creation on DZ datasources'
            description=data_source_description,
            # insert the domain identifier corresponding to the domain to which the
 datasource will belong, example: domainIdentifier= 'dzd_6f3gst5jjmrrmv'
            domainIdentifier=domain_id,
            # give environment identifier , example: environmentIdentifier=
 '3weyt6hhn8qcvb'
            environmentIdentifier=environment_id,
            # give corresponding project identifier, example: projectIdentifier=
 '6tl4csoyrg16ef',
            projectIdentifier=project_id,
            enableSetting="ENABLED",
            # publishOnImport used to select whether assets are added to the inventory
 and/or discovery catalog .
            # publishOnImport = True : Assets will be added to project's inventory as
 well as published to the discovery catalog
            # publishOnImport = False : Assets will only be added to project's
 inventory.
            # You can later curate the metadata of the assets and choose subscription
 terms to publish them from the inventory to the discovery catalog.
            publishOnImport=False,
            # Automated business name generation : Use AI to automatically generate
 metadata for assets as they are published or updated by this data source run.
            # Automatically generated metadata can be be approved, rejected, or edited
 by data publishers.
            # Automatically generated metadata is badged with a small icon next to the
 corresponding metadata field.
            recommendation={"enableBusinessNameGeneration": True},
            type="GLUE",
            configuration={
                "glueRunConfiguration": {
                    "dataAccessRole": "arn:aws:iam::"
                    + account_id
                    + ":role/service-role/AmazonDataZoneGlueAccess-"
                    + current_region
```

```
                    + "-"
                    + domain_id
                    + "",
                    "relationalFilterConfigurations": [
                        {
                            #
                            "databaseName": glue_database_name,
                            "filterExpressions": [
                                {"expression": "*", "type": "INCLUDE"},
                            ],
                            #    "schemaName": "TestSchemaName",
                        },
                    ],
                },
            },
            # Add metadata forms to the data source (OPTIONAL).
            # Metadata forms will be automatically applied to any assets that are
 created by the data source.
            # assetFormsInput=[
            #     {
            #         "content": "string",
            #         "formName": "string",
            #         "typeIdentifier": "string",
            #         "typeRevision": "string",
            #     },
            # ],
            schedule={
                "schedule": "cron(5 20 * * ? *)",
                "timezone": "UTC",
            },
        )
        # This is a suggested syntax to return values
        #       return_values["data_source_creation"] = data_source_creation["items"]
        print("Data Source Created")


//This is the sample response payload after the CreateDataSource API is invoked:

{
    "Content":{
        "project_name": "Admin",
        "domain_name": "Drug-Research-and-Development",
        "env_name": "GlueEnvironment",
        "glue_database_name": "test",
```

```
        "data_source_name" : "test",
        "data_source_description" : "This is a test data source"
    }
}
```

데이터 자산 큐레이션 및 게시

다음 샘플 스크립트를 사용하여 DataZone Amazon에서 데이터 자산을 큐레이션하고 게시할 수 있습니다.

다음 스크립트를 사용하여 사용자 지정 양식 유형을 생성할 수 있습니다.

```
def create_form_type(domainId, projectId):
    return dzclient.create_form_type(
        domainIdentifier = domainId,
        name = "customForm",
        model = {
            "smithy": "structure customForm { simple: String }"
        },
        owningProjectIdentifier = projectId,
        status = "ENABLED"
    )
```

다음 샘플 스크립트를 사용하여 사용자 지정 에셋 유형을 만들 수 있습니다.

```
def create_custom_asset_type(domainId, projectId):
    return dzclient.create_asset_type(
        domainIdentifier = domainId,
        name = "userCustomAssetType",
        formsInput = {
            "Model": {
                "typeIdentifier": "customForm",
                "typeRevision": "1",
                "required": False
            }
        },
        owningProjectIdentifier = projectId,
    )
```

다음 샘플 스크립트를 사용하여 커스텀 에셋을 만들 수 있습니다.

```
def create_custom_asset(domainId, projectId):
    return dzclient.create_asset(
        domainIdentifier = domainId,
        name = 'custom asset',
        description = "custom asset",
        owningProjectIdentifier = projectId,
        typeIdentifier = "userCustomAssetType",
        formsInput = [
            {
                "formName": "UserCustomForm",
                "typeIdentifier": "customForm",
                "content": "{\"simple\":\"sample-catalogId\"}"
            }
        ]
    )
```

다음 샘플 스크립트를 사용하여 용어집을 만들 수 있습니다.

```
def create_glossary(domainId, projectId):
    return dzclient.create_glossary(
        domainIdentifier = domainId,
        name = "test7",
        description = "this is a test glossary",
        owningProjectIdentifier = projectId
    )
```

다음 샘플 스크립트를 사용하여 용어집 용어를 만들 수 있습니다.

```
def create_glossary_term(domainId, glossaryId):
    return dzclient.create_glossary_term(
        domainIdentifier = domainId,
        name = "soccer",
        shortDescription = "this is a test glossary",
```

```
        glossaryIdentifier = glossaryId,
    )
```

다음 샘플 스크립트를 사용하여 시스템 정의 자산 유형을 사용하여 자산을 만들 수 있습니다.

```
def create_asset(domainId, projectId):
    return dzclient.create_asset(
        domainIdentifier = domainId,
        name = 'sample asset name',
        description = "this is a glue table asset",
        owningProjectIdentifier = projectId,
        typeIdentifier = "amazon.datazone.GlueTableAssetType",
        formsInput = [
            {
                "formName": "GlueTableForm",
                "content": "{\"catalogId\":\"sample-catalogId\",\"columns\":
[{\"columnDescription\":\"sample-columnDescription\",\"columnName\":\"sample-
columnName\",\"dataType\":\"sample-dataType\",\"lakeFormationTags\":{\"sample-
key1\":\"sample-value1\",\"sample-key2\":\"sample-value2\"}}],\"compressionType\":
\"sample-compressionType\",\"lakeFormationDetails\":{\"lakeFormationManagedTable
\":false,\"lakeFormationTags\":{\"sample-key1\":\"sample-value1\",\"sample-key2\":
\"sample-value2\"}},\"primaryKeys\":[\"sample-Key1\",\"sample-Key2\"],\"region\":
\"us-east-1\",\"sortKeys\":[\"sample-sortKey1\"],\"sourceClassification\":\"sample-
sourceClassification\",\"sourceLocation\":\"sample-sourceLocation\",\"tableArn\":
\"sample-tableArn\",\"tableDescription\":\"sample-tableDescription\",\"tableName\":
\"sample-tableName\"}"
            }
        ]
    )
```

다음 샘플 스크립트를 사용하여 에셋 리비전을 생성하고 용어집 용어를 첨부할 수 있습니다.

```
def create_asset_revision(domainId, assetId):
    return dzclient.create_asset_revision(
        domainIdentifier = domainId,
        identifier = assetId,
        name = 'glue table asset 7',
        description = "glue table asset description update",
        formsInput = [
```

```
            {
                "formName": "GlueTableForm",
                "content": "{\"catalogId\":\"sample-catalogId\",\"columns\":
[{\"columnDescription\":\"sample-columnDescription\",\"columnName\":\"sample-
columnName\",\"dataType\":\"sample-dataType\",\"lakeFormationTags\":{\"sample-
key1\":\"sample-value1\",\"sample-key2\":\"sample-value2\"}}],\"compressionType\":
\"sample-compressionType\",\"lakeFormationDetails\":{\"lakeFormationManagedTable
\":false,\"lakeFormationTags\":{\"sample-key1\":\"sample-value1\",\"sample-key2\":
\"sample-value2\"}},\"primaryKeys\":[\"sample-Key1\",\"sample-Key2\"],\"region\":
\"us-east-1\",\"sortKeys\":[\"sample-sortKey1\"],\"sourceClassification\":\"sample-
sourceClassification\",\"sourceLocation\":\"sample-sourceLocation\",\"tableArn\":
\"sample-tableArn\",\"tableDescription\":\"sample-tableDescription\",\"tableName\":
\"sample-tableName\"}"
            }
        ],
        glossaryTerms = ["<glossaryTermId:>"]
    )
```

다음 샘플 스크립트를 사용하여 자산을 게시할 수 있습니다.

```
def publish_asset(domainId, assetId):
    return dzclient.create_listing_change_set(
        domainIdentifier = domainId,
        entityIdentifier = assetId,
        entityType = "ASSET",
        action = "PUBLISH",
    )
```

데이터 카탈로그 검색 및 데이터 구독

다음 샘플 스크립트를 사용하여 데이터 카탈로그를 검색하고 데이터를 구독할 수 있습니다.

```
def search_asset(domainId, projectId, text):
    return dzclient.search(
        domainIdentifier = domainId,
        owningProjectIdentifier = projectId,
        searchScope = "ASSET",
        searchText = text,
    )
```

다음 샘플 스크립트를 사용하여 자산의 리스팅 ID를 가져올 수 있습니다.

```
def search_listings(domainId, assetName, assetId):
    listings = dzclient.search_listings(
        domainIdentifier=domainId,
        searchText=assetName,
        additionalAttributes=["FORMS"]
    )

    assetListing = None
    for listing in listings['items']:
        if listing['assetListing']['entityId'] == assetId:
            assetListing = listing

    return listing['assetListing']['listingId']
```

다음 샘플 스크립트를 사용하여 리스팅 ID를 사용하여 구독 요청을 생성할 수 있습니다.

```
create_subscription_response = def create_subscription_request(domainId, projectId,
 listingId):
    return dzclient.create_subscription_request(
        subscribedPrincipals=[{
            "project": {
                "identifier": projectId
            }
        }],
        subscribedListings=[{
            "identifier": listingId
        }],
        requestReason="Give request reason here."
    )
```

`create_subscription_response`위의 내용을 사용하여 다음 샘플 스크립트를 `subscription_request_id` 사용하여 구독을 받은 다음 구독을 수락/승인합니다.

```
subscription_request_id = create_subscription_response["id"]

def accept_subscription_request(domainId, subscriptionRequestId):
    return dzclient.accept_subscription_request(
        domainIdentifier=domainId,
        identifier=subscriptionRequestId
    )
```

기타 유용한 샘플 스크립트

Amazon에서 데이터를 작업할 때 다음 샘플 스크립트를 사용하여 다양한 작업을 완료할 수 DataZone 있습니다.

다음 샘플 스크립트를 사용하여 기존 Amazon DataZone 도메인을 나열하십시오.

```
def list_domains():
    datazone = boto3.client('datazone')
    response = datazone.list_domains(status='AVAILABLE')
    [print("%12s | %16s | %12s | %52s" % (item['id'], item['name'],
 item['managedAccountId'], item['portalUrl'])) for item in response['items']]
    return
```

다음 샘플 스크립트를 사용하여 기존 Amazon DataZone 프로젝트를 나열하십시오.

```
def list_projects(domain_id):
    datazone = boto3.client('datazone')
    response = datazone.list_projects(domainIdentifier=domain_id)
    [print("%12s | %16s " % (item['id'], item['name'])) for item in response['items']]
    return
```

다음 샘플 스크립트를 사용하여 기존 Amazon DataZone 메타데이터 양식을 나열하십시오.

```
def list_metadata_forms(domain_id):
    datazone = boto3.client('datazone')
    response = datazone.search_types(domainIdentifier=domain_id,
```

```
        managed=False,
        searchScope='FORM_TYPE')
    [print("%16s | %16s | %3s | %8s" % (item['formTypeItem']['name'],
item['formTypeItem']['owningProjectId'],item['formTypeItem']['revision'],
item['formTypeItem']['status'])) for item in response['items']]
    return
```

Amazon DataZone 도메인 및 사용자 액세스 관리

주제

도메인 생성

> **Note**
>
> Amazon을 AWS Identity DataZone Center와 함께 사용하여 SSO 사용자 및 그룹에 대한 액세스 권한을 제공하는 경우 현재 Amazon DataZone 도메인은 AWS ID 센터 인스턴스와 동일한 AWS 지역에 있어야 합니다.

DataZoneAmazon이라는 도메인은 자산, 사용자 및 프로젝트를 함께 연결하는 조직 조직입니다. 자세한 정보는 아마존 DataZone 용어 및 개념을 참조하세요.

Amazon DataZone 도메인을 생성하려면 관리자 권한이 있는 계정에서 IAM 역할을 수임해야 합니다. Amazon DataZone 관리 콘솔을 사용하는 데 필요한 IAM 권한을 구성합니다.도메인을 생성하는 데 필요한 최소 권한을 얻으려면

Amazon이 기본 구성으로 도메인 사용자를 대신하여 작업을 DataZone 수행하려면 추가 IAM 역할이 필요합니다. 이러한 IAM 역할을 미리 생성하거나 Amazon에서 자동으로 DataZone 생성하도록 할 수 있습니다. Amazon이 도메인 생성 프로세스 중에 이러한 IAM 역할을 대신 DataZone 생성하도록 하려면 도메인을 생성하려면 역할 생성 권한이 있는 IAM 역할을 맡아야 합니다. Amazon DataZone 서비스 콘솔의 간소화된 역할 생성을 활성화하기 위해 IAM 권한에 대한 사용자 지정 정책을 생성합니다.를 참조하세요. 도메인 생성 선택에 따라 DataZone Amazon은 최대 4개의 새 IAM 역할 (AmazonDataZoneDomainExecutionRole,

AmazonDataZoneGlueManageAccessRoleAmazonDataZoneRedshiftManageAccessRole, 및 AmazonDataZoneProvisioningRole) 을 생성합니다.

Amazon DataZone 도메인을 생성하려면 다음 절차를 완료하십시오.

1. https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동한 다음 상단 탐색 표시줄의 지역 선택기를 사용하여 적절한 AWS 지역을 선택합니다.
2. 도메인 생성을 선택하고 다음 필드에 값을 입력합니다.

   - 이름 - 도메인에 친숙한 이름을 지정합니다. 도메인을 생성한 후에는 이 이름을 변경할 수 없습니다.
   - 설명 - (선택 사항) 도메인 설명을 지정합니다.
   - 데이터 암호화 - Amazon DataZone 도메인, 메타데이터 및 보고 데이터는 Amazon DataZone 전용 AWS 키를 사용하여 KMS (키 관리 서비스) 에 의해 암호화됩니다. 이 필드를 사용하여 AWS 소유 키를 사용할지 아니면 다른 AWS KMS 키를 선택할지를 지정합니다.

     고객 관리 키 사용에 대한 자세한 내용은 을 참조하십시오Amazon의 유휴 데이터 암호화 DataZone. 데이터 암호화에 자체 KMS 키를 사용하는 경우 AmazonDataZoneDomainExecutionRole 기본값에 다음 설명을 포함해야 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:GenerateDataKey"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

- 서비스 액세스 - Amazon에서 새 DomainExecutionRoleIAM 역할을 DataZone 생성하여 사용하도록 할지 아니면 기존 IAM 역할을 선택할지 선택합니다.
- 빠른 설정 - (선택 사항) Amazon에서 데이터 소비 및 게시를 위한 계정을 DataZone 설정하여 더 빠르게 시작하려면 이 확인란을 선택하십시오. DataZone Amazon은 AWS Glue 및 Amazon Redshift 리소스에 대한 액세스를 프로비저닝, 수집 및 관리하기 위한 세 가지 IAM 역할을 생성하고, 새 Amazon S3 버킷을 생성하고, Amazon 관리 DataZone 프로젝트를 생성하고, 데이터 레이크와 데이터 웨어하우스 기본 청사진에 대한 환경 프로필을 생성합니다.
- 태그 - (선택 사항) 도메인의 AWS 태그 (키 및 값 쌍) 를 지정합니다.
- 도메인이 성공적으로 생성되면 브라우저를 새로 고쳐 새 Amazon DataZone 도메인의 세부 정보 페이지를 표시해야 합니다.

도메인 편집

Amazon에서 도메인은 자산 DataZone, 사용자 및 프로젝트를 함께 연결하는 조직 엔티티입니다. 자세한 정보는 아마존 DataZone 용어 및 개념을 참조하세요.

Amazon DataZone 도메인을 생성한 후 나중에 설명을 변경하고, IAM Identity Center를 활성화하고, 태그 키와 해당 값을 추가, 편집 또는 제거하도록 도메인을 편집할 수 있습니다. Amazon DataZone 도메인을 편집하려면 관리자 권한이 있는 계정에서 IAM 역할을 수임해야 합니다. Amazon DataZone 관리 콘솔을 사용하는 데 필요한 IAM 권한을 구성합니다.도메인을 편집하는 데 필요한 최소 권한을 얻으려면

도메인을 편집하려면 다음 단계를 완료하세요.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔을 엽니다.
2. 도메인 보기를 선택하고 목록에서 도메인 이름을 선택합니다. 이름은 하이퍼링크입니다.
3. 도메인의 세부정보 페이지에서 편집을 선택합니다.
4.
   - 설명을 편집합니다.
   - IAM ID 센터 설정을 설정합니다. 이러한 설정에 대한 자세한 내용은 을 참조하십시오. 아마존용 AWS IAM 아이덴티티 센터 설정 DataZone
   - 태그 키와 해당 값을 추가, 편집 또는 제거합니다.
5. 편집한 후 도메인 업데이트를 선택합니다.

도메인 삭제

Amazon에서 도메인은 자산 DataZone, 사용자 및 프로젝트를 함께 연결하는 조직 엔티티입니다. 자세한 정보는 아마존 DataZone 용어 및 개념을 참조하세요.

도메인 삭제 행위는 최종적입니다. 삭제하면 데이터 소스, 프로젝트, 환경, 자산, 용어집, 메타데이터 양식 등 모든 Amazon DataZone 개체가 영구적으로 제거됩니다. 삭제해도 IAM 역할, S3 버킷, AWS Glue 데이터베이스, Redshift를 통한 구독 권한 부여 등 Amazon에서 생성하는 데 도움을 준 Amazon DataZone 이외의 DataZone AWS 리소스는 삭제되지 않습니다. LakeFormation 이러한 리소스가 더 이상 필요하지 않은 경우 해당 서비스에서 삭제하십시오. AWS

다른 사람이 악의적으로 도메인을 삭제하는 것을 방지하려면 도메인을 삭제하려면 DataZone Amazon에 대한 관리자 IAM 권한이 필요합니다. 이 권한은 IAM으로 구성할 수 있습니다. 실수로 도메인을 삭제하는 것을 방지하려면 Amazon DataZone 콘솔에서 도메인을 삭제하려면 확인 단어가 필요합니다.

도메인을 삭제하려면 다음 단계를 완료하십시오.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔을 엽니다.
2. 도메인 보기를 선택하고 목록에서 도메인 이름을 선택합니다. 이름은 하이퍼링크입니다.
3. [Delete] 를 선택하고 정보 경고를 검토하십시오.
4. 요청된 텍스트를 입력하여 이러한 경고를 이해했는지 확인하십시오. 삭제를 선택합니다.

> **Important**
>
> 도메인 삭제는 취소할 수 없으며 본인 또는 본인이 직접 취소할 수 없습니다. AWS

> **Note**
>
> 귀하 또는 도메인 사용자가 프로젝트에 환경을 만들면 Amazon은 도메인 또는 관련 계정에 AWS 리소스를 DataZone 생성하여 귀하와 귀하의 도메인 사용자에게 기능을 제공합니다. 다음은 Amazon이 도메인의 프로젝트를 위해 생성할 DataZone 수 있는 AWS 리소스 목록과 기본 이름입니다. 도메인을 삭제해도 AWS 계정에서 이러한 AWS 리소스는 삭제되지 않습니다.
>
> - <environmentId>IAM 역할: 데이터존_usr_.
> - <environmentName>글루 데이터베이스: (1) <environmentName>_pub_db-*, (2) _sub_db-*. 이 이름의 기존 데이터베이스가 이미 있는 경우 DataZone Amazon은 환경 ID를 추가합니다.

- <environmentName>Athena 워크그룹: -*. 이 이름의 기존 워크그룹이 이미 있는 경우 DataZone Amazon은 환경 ID를 추가합니다.
- CloudWatch 로그 그룹: 데이터존_ <environmentId>

Amazon용 IAM 자격 증명 센터 활성화 DataZone

> **Note**
>
> 이 절차를 완료하려면 Amazon DataZone 도메인과 동일한 AWS 지역에서 AWS IAM ID 센터를 활성화해야 합니다.

AWS IAM ID 센터를 사용하여 SSO 사용자 및 그룹에 Amazon DataZone 데이터 포털에 대한 액세스 권한을 제공할 수 있습니다. 완료 아마존용 AWS IAM 아이덴티티 센터 설정 DataZone 후 SSO 사용자 및 그룹이 Amazon DataZone 도메인 데이터 포털에 액세스할 수 있도록 설정할 수 있습니다.

Amazon DataZone 도메인에서 AWS IAM ID 센터를 사용할 수 있게 하려면 관리자 권한이 있는 계정에서 IAM 역할을 수임해야 합니다. Amazon DataZone 관리 콘솔을 사용하는 데 필요한 IAM 권한을 구성합니다. DataZoneAmazon에서 사용할 수 있도록 IAM ID 센터를 활성화하는 데 필요한 최소 권한을 확보해야 합니다. Amazon DataZone 서비스 콘솔의 간소화된 역할 생성을 활성화하기 위해 IAM 권한에 대한 사용자 지정 정책을 생성합니다.

DataZoneAmazon용 AWS IAM ID 센터를 활성화하려면 다음 절차를 완료하십시오.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/datazone 에서 DataZone 콘솔을 엽니다.
2. 도메인 보기를 선택하고 목록에서 도메인 이름을 선택합니다. 이름은 하이퍼링크입니다.
3. 도메인의 세부 정보 페이지에서 편집을 선택합니다.
   - IAM ID 센터에서 사용자 활성화 확인란을 선택합니다.
   - 두 가지 사용자 할당 모드 중에서 선택합니다. 선택한 도메인으로 도메인을 업데이트한 후에는 변경할 수 없습니다.
     - 암시적 사용자 할당을 사용하면 IAM ID 센터 디렉터리에 추가된 모든 사용자가 Amazon DataZone 도메인에 액세스할 수 있습니다.

- 명시적 사용자 할당을 사용하면 IAM Identity Center 디렉터리의 특정 사용자 또는 그룹을 추가하여 Amazon DataZone 도메인에 대한 액세스를 제공할 수 있습니다. 나중에 Amazon DataZone Console에서 이러한 사용자 및 그룹을 추가하고 제거하게 됩니다.

4. 선택에 만족하면 도메인 업데이트를 선택합니다.

Amazon용 IAM 자격 증명 센터 비활성화 DataZone

Amazon DataZone 도메인의 AWS IAM ID 센터를 비활성화하면 모든 SSO 사용자의 액세스 권한이 제거됩니다.

> **Note**
>
> IAM ID 센터를 비활성화해도 SSO 사용자에 대한 요금 청구는 중단되지 않습니다. SSO 사용자에 대한 요금 청구를 중지하려면 도메인에서 해당 사용자를 비활성화해야 합니다. 청구는 사용자가 비활성화된 달의 말일까지 계속됩니다. 사용자를 비활성화하려면 을 참조하십시오. Amazon DataZone 콘솔에서 사용자 관리

AWS IAM ID 센터를 사용하여 SSO 사용자 및 그룹에 Amazon DataZone 데이터 포털에 대한 액세스 권한을 제공할 수 있습니다. DataZoneAmazon용 AWS IAM ID 센터를 활성화한 경우 나중에 모든 사용자에 대한 액세스를 비활성화할 수 있습니다.

Amazon DataZone 도메인에서 사용할 수 있도록 AWS IAM ID 센터를 비활성화하려면 관리자 권한이 있는 계정에서 IAM 역할을 수임해야 합니다. Amazon DataZone 관리 콘솔을 사용하는 데 필요한 IAM 권한을 구성합니다. DataZoneAmazon에서 IAM ID 센터를 사용하지 못하도록 하는 데 필요한 최소 권한을 확보해야 합니다. Amazon DataZone 서비스 콘솔의 간소화된 역할 생성을 활성화하기 위해 IAM 권한에 대한 사용자 지정 정책을 생성합니다.

DataZoneAmazon용 AWS IAM ID 센터를 비활성화하려면 다음 절차를 완료하십시오.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/datazone 에서 DataZone 콘솔을 엽니다.
2. 도메인 보기를 선택하고 목록에서 도메인 이름을 선택합니다. 이름은 하이퍼링크입니다.
3. <regionName><accountId><domainName>arn:aws:datazone: ::도메인/으로 시작하는 도메인의 Amazon 리소스 이름 (ARN) 을 복사합니다.
4. https://console.aws.amazon.com/singlesignon/ 에서 IAM 아이덴티티 센터 콘솔을 엽니다.
5. [Applications]를 선택합니다.

6. AWS IAM Identity Center를 비활성화하려는 도메인을 선택합니다. 비활성화하면 모든 SSO 사용자의 도메인 데이터 포털 액세스 권한이 제거됩니다. 필터 메뉴와 검색 상자를 사용하여 애플리케이션 목록을 필터링할 수 있습니다.
7. 작업 메뉴에서 비활성화를 선택합니다.
8. SSO 사용자는 Amazon DataZone 도메인에 액세스할 수 없게 됩니다.
9. Amazon DataZone 도메인에 대해 AWS IAM ID 센터를 다시 활성화하려면 AWS IAM ID 센터를 다시 활성화하려는 도메인을 선택하고 작업 메뉴에서 활성화를 선택합니다.

Amazon DataZone 콘솔에서 사용자 관리

사용자는 자격 AWS 증명 또는 싱글 사인온 (SSO) 자격 증명을 사용하여 Amazon DataZone 데이터 포털에 액세스할 수 있습니다. Amazon DataZone 도메인의 Amazon DataZone 콘솔에서 사용자를 관리하려면 관리자 권한이 있는 계정의 IAM 역할을 수임해야 합니다. Amazon DataZone 관리 콘솔을 사용하는 데 필요한 IAM 권한을 구성합니다.Amazon DataZone 콘솔에서 사용자를 관리하는 데 필요한 최소 권한을 확보해야 합니다.

주제

- IAM 역할 및 사용자 관리
- SSO 사용자 관리
- SSO 그룹 관리

IAM 역할 및 사용자 관리

IAM 역할 및 사용자는 AWS ID 및 액세스 관리 (IAM) 를 사용하여 생성되며 정책을 통해 부여된 권한을 통해 Amazon DataZone 도메인에 액세스할 수 있습니다. 자세한 정보는 Amazon DataZone 데이터 포털을 사용하는 데 필요한 IAM 권한을 구성합니다.을 참조하세요. Amazon DataZone 도메인 구독을 활성화한 IAM 역할 및 사용자 목록을 보고, 액세스를 비활성화하고, 이전에 비활성화한 경우 액세스를 활성화할 수 있습니다.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/datazone 에서 DataZone 콘솔을 엽니다.
2. 도메인 보기를 선택하고 목록에서 도메인 이름을 선택합니다. 이름은 하이퍼링크입니다.
3. 도메인의 세부정보 페이지에서 사용자 관리를 선택합니다.
4. 사용자 유형에서 IAM 사용자를 선택하면 활성화되거나 비활성화된 IAM 사용자 및 역할의 현재 목록을 볼 수 있습니다.

- 이름 열에는 IAM 사용자 또는 역할의 arn이 표시됩니다.
- 상태 열에는 도메인 내 IAM 사용자 또는 역할의 현재 상태가 표시됩니다.
  - 활성화됨이란 IAM 사용자 또는 역할이 API를 호출하거나 명령줄 인터페이스를 통해 명령을 실행했거나 도메인의 Amazon DataZone 포털에 액세스했음을 의미하며, 해당 사용자의 구독 요금이 청구됩니다.
  - 비활성화됨은 IAM 사용자 또는 역할의 Amazon DataZone 도메인에 대한 액세스가 차단되었음을 의미합니다.

5. 현재 활성화된 IAM 사용자 또는 역할을 비활성화하려면 사용자 옆의 체크박스를 선택하고 작업 메뉴에서 비활성화를 선택합니다. 사용자는 Amazon DataZone 도메인에 액세스할 수 없게 됩니다. 사용자에 대한 청구는 이번 달 말에 종료됩니다.
6. 현재 비활성화된 IAM 사용자 또는 역할을 활성화하려면 사용자 옆의 체크박스를 선택하고 작업 메뉴에서 활성화를 선택합니다. IAM 사용자 또는 역할에 적절한 권한이 있는 경우 사용자는 Amazon DataZone 도메인에 액세스할 수 있습니다. 사용자에 대한 청구가 다시 시작됩니다.

SSO 사용자 관리

SSO 사용자는 AWS IAM ID 센터에서 ID 공급자와 생성되거나 동기화됩니다. 자세한 내용은 DataZone Amazon용 AWS IAM ID 센터 활성화 및 구성을 참조하십시오아마존용 AWS IAM 아이덴티티 센터 설정 DataZone. Amazon용 IAM 자격 증명 센터 활성화 DataZone 도메인에 할당된 SSO 사용자 목록을 보고, SSO 사용자를 추가하고, SSO 사용자를 제거할 수 있습니다.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/datazone 에서 DataZone 콘솔을 엽니다.
2. 도메인 보기를 선택하고 목록에서 도메인 이름을 선택합니다. 이름은 하이퍼링크입니다.
3. 도메인의 세부정보 페이지에서 아래로 스크롤하여 사용자 관리를 선택합니다.
4. 사용자 유형에서 SSO 사용자를 선택하면 현재 SSO 사용자 목록을 볼 수 있습니다.

- 이름 열에는 SSO 사용자 이름이 표시됩니다.
- 상태 열에는 도메인에 있는 SSO 사용자의 현재 상태가 표시됩니다.
  - 할당됨은 SSO 사용자가 도메인에 명시적으로 할당되었음을 의미합니다. 따라서 사용자는 Amazon에 액세스할 수 DataZone 있습니다. 이 상태는 도메인의 ID 제공자 모드가 명시적 할당으로 설정된 경우에만 사용됩니다.
  - 활성화됨은 SSO 사용자가 해당 도메인의 Amazon DataZone 포털에 액세스했으며 해당 사용자의 구독 요금이 청구되었음을 의미합니다. 활성화는 자동으로 이루어집니다.

- 비활성화됨이란 도메인의 데이터 포털에 대한 SSO 사용자 액세스가 차단되었음을 의미합니다. 해당 사용자에 대한 청구는 액세스가 비활성화된 월말에 종료되었습니다.
- 제거란 SSO 사용자가 이전에 도메인에 배정되었지만 액세스하기 전에 제거되었음을 의미합니다.

5. 사용자 추가 및 추가를 선택하여 SSO 사용자를 추가합니다. 도메인이 암시적 사용자 할당으로 설정된 경우 이 옵션을 사용할 수 없습니다. 즉, 자격 증명 풀의 모든 사용자가 Amazon DataZone 도메인에 액세스할 수 있습니다.

   - 사용자 추가 페이지에서 추가하려는 사용자의 별칭을 검색합니다. 검색 상자 아래에 일치 가능성이 있는 목록이 표시됩니다.
   - 추가하려는 사용자를 선택합니다. 사용자의 별칭은 검색 상자 아래에 칩 모양으로 표시됩니다.
   - 추가하려는 사용자 목록에 만족하면 사용자 추가를 선택합니다.
   - 사용자는 할당됨 상태인 Amazon DataZone 도메인에 배정됩니다.
   - 사용자가 도메인의 데이터 포털에 처음 액세스하면 상태가 자동으로 활성화됨으로 변경되고 사용자 구독 요금이 청구되기 시작합니다.
6. 사용자를 선택하고 작업 메뉴에서 비활성화를 선택하여 할당된 SSO 사용자를 제거합니다. 따라서 사용자는 Amazon DataZone 도메인에 액세스할 수 없게 됩니다. 사용자 상태는 제거됨으로 표시됩니다. 도메인이 암시적 사용자 할당으로 설정된 경우에는 이 옵션을 사용할 수 없습니다.
7. 사용자를 선택하고 작업 메뉴에서 비활성화를 선택하여 활성화된 SSO 사용자를 비활성화합니다. 따라서 Amazon DataZone 도메인에 대한 사용자 액세스가 손실되고 차단됩니다. 해당 월말까지 사용자 구독에 대한 청구가 계속됩니다. 사용자 상태는 비활성화됨으로 표시됩니다.
8. 사용자를 선택하고 작업 메뉴에서 활성화를 선택하여 비활성화된 SSO 사용자를 활성화합니다. 따라서 사용자는 Amazon DataZone 도메인에 다시 액세스할 수 있게 됩니다. 청구는 즉시 시작됩니다. 사용자의 계정이 활성화됨으로 표시됩니다.

SSO 그룹 관리

SSO 그룹은 AWS IAM ID 센터에서 ID 공급자와 생성되거나 동기화됩니다. 자세한 내용은 DataZone Amazon용 AWS IAM ID 센터 활성화 및 구성을 참조하십시오아마존용 AWS IAM 아이덴티티 센터 설정 DataZone. Amazon용 IAM 자격 증명 센터 활성화 DataZone 도메인에 할당된 SSO 그룹 목록을 보고, SSO 그룹을 추가하고, SSO 그룹을 제거할 수 있습니다.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/datazone 에서 DataZone 콘솔을 엽니다.
2. 도메인 보기를 선택하고 목록에서 도메인 이름을 선택합니다. 이름은 하이퍼링크입니다.

3. 도메인의 세부정보 페이지에서 아래로 스크롤하여 사용자 관리를 선택합니다.
4. 사용자 유형에서 SSO 그룹을 선택하면 SSO 그룹의 현재 목록을 볼 수 있습니다.

   - 이름 열에는 SSO 그룹 이름이 표시됩니다.
   - 상태 열에는 도메인에 있는 SSO 그룹의 현재 상태가 표시됩니다.
     - 할당됨은 SSO 그룹이 도메인에 명시적으로 할당되었음을 의미합니다. 따라서 그룹의 모든 사용자는 도메인의 데이터 포털에 접근할 수 있습니다 (사용자가 비활성화되지 않은 경우).
     - 할당되지 않음은 SSO 그룹이 도메인에서 제거되었음을 의미합니다. 그룹의 사용자는 이 그룹의 구성원 자격을 통해 도메인의 데이터 포털에 접근할 수 없습니다.
5. 그룹 추가 및 추가를 선택하여 SSO 그룹을 추가합니다. 도메인이 암시적 사용자 할당으로 설정된 경우 이 옵션을 사용할 수 없습니다. 즉, 자격 증명 풀의 모든 사용자는 그룹 멤버십에 관계없이 Amazon DataZone 도메인에 액세스할 수 있습니다.

   - 그룹 추가 페이지에서 추가하려는 그룹의 별칭을 검색합니다. 검색 상자 아래에 일치 가능성이 있는 목록이 표시됩니다.
   - 추가하려는 그룹을 선택합니다. 해당 별칭은 검색 상자 아래에 칩 모양으로 표시됩니다.
   - 추가하려는 그룹 목록에 만족하면 그룹 추가를 선택합니다.
   - 그룹은 Assited라는 상태의 Amazon DataZone 도메인에 할당됩니다.
   - 그룹 구성원이 도메인의 데이터 포털에 액세스하면 상태가 자동으로 활성화됨으로 변경되고 사용자 구독에 대한 요금이 청구되기 시작합니다.
6. 그룹을 선택하고 작업 메뉴에서 할당 취소를 선택하여 할당된 SSO 그룹을 제거합니다. 따라서 그룹은 Amazon DataZone 도메인에 대한 액세스 권한을 잃게 됩니다. 그룹 상태는 할당되지 않음으로 표시됩니다. 이 그룹의 멤버십을 DataZone 통해 Amazon에 대한 액세스 권한을 얻은 사용자는 액세스 권한을 잃게 됩니다. 도메인이 암시적 사용자 할당으로 설정된 경우에는 이 옵션을 사용할 수 없습니다. 그룹 할당을 취소하여 액세스 권한이 제거된 사용자에 대한 요금 청구를 중지하려면 다음으로 사용자 프로필을 수동으로 선택하고 비활성화해야 합니다.

Amazon DataZone 데이터 포털에서의 사용자 권한 관리

Amazon의 현재 릴리스에서는 기본 권한 부여 메커니즘을 통해 Amazon DataZone 도메인의 모든 인증된 사용자 (IAM 및 SSO) 가 프로젝트를 생성하고 DataZone, 프로젝트 내에 엔티티를 만들고, 검색을 수행할 수 있습니다. 프로젝트 구성원은 여전히 지정된 프로젝트 소유자 또는 프로젝트 기여자 역할에 따라 자신에게 부여된 권한을 준수해야 합니다.

Amazon DataZone 내장 블루프린트로 작업하기

환경을 만드는 블루프린트는 환경이 속한 프로젝트의 구성원이 Amazon DataZone 카탈로그의 자산을 사용할 때 사용할 수 있는 도구 및 서비스를 정의합니다. DataZoneAmazon의 현재 릴리스에는 다음과 같은 기본 제공 블루프린트가 있습니다.

- 데이터 레이크 블루프린트
- 데이터 웨어하우스 청사진
- 아마존 SageMaker 블루프린트

주제

Amazon 도메인을 소유한 AWS 계정에서 빌트인 블루프린트를 활성화합니다. DataZone

환경을 만드는 블루프린트는 환경이 속한 프로젝트의 구성원이 Amazon DataZone 카탈로그의 자산을 사용할 때 사용할 수 있는 도구 및 서비스를 정의합니다.

Amazon의 현재 릴리스에는 데이터 레이크 청사진 DataZone, 데이터 웨어하우스 청사진, Amazon 청사진 등 여러 가지 기본 제공 청사진이 있습니다. SageMaker

- 데이터 레이크 블루프린트에는 Amazon 카탈로그에 데이터 레이크 자산을 게시하고 사용하기 위한 일련의 서비스 (AWS Glue, AWS Lake Formation, Amazon Athena) 를 시작하고 구성하는 데 대한 정의가 포함되어 있습니다. DataZone
- 데이터 웨어하우스 블루프린트에는 아마존 카탈로그에 Amazon Redshift 자산을 게시하고 사용하기 위한 서비스 세트 (Amazon Redshift) 를 시작하고 구성하는 데 대한 정의가 포함되어 있습니다. DataZone
- Amazon SageMaker Blueprint에는 Amazon DataZone 카탈로그에 Amazon SageMaker 자산을 게시하고 사용하기 위한 서비스 세트 (Amazon SageMaker Studio) 를 시작하고 구성하는 데 대한 정의가 포함되어 있습니다.

자세한 정보는 아마존 DataZone 용어 및 개념을 참조하세요.

Amazon DataZone 도메인을 생성할 때 기본 데이터 레이크와 기본 데이터 웨어하우스 내장 블루프린트를 도메인 생성 프로세스의 일부로 자동으로 활성화하는 빠른 설정을 선택할 수 있습니다. 또한 Quick Setup은 이러한 내장된 블루프린트를 사용하여 기본 환경 프로필과 기본 환경을 생성합니다.

Amazon 도메인을 생성할 때 빠른 설정을 선택하지 않는 경우, 아래 절차에 따라 이 Amazon DataZone DataZone 도메인이 있는 AWS 계정에서 사용 가능한 빌트인 블루프린트를 활성화할 수 있습니다. 이러한 빌트인 블루프린트를 활성화해야 이 도메인에서 환경 프로파일과 환경을 생성하는 데 사용할 수 있습니다.

Amazon DataZone 관리 콘솔을 통해 Amazon DataZone 도메인에 내장된 블루프린트를 활성화하려면 관리자 권한이 있는 계정에서 IAM 역할을 수임해야 합니다. Amazon DataZone 관리 콘솔을 사용하는 데 필요한 IAM 권한을 구성합니다.최소 권한을 얻으려면

Amazon DataZone 도메인에서 빌트인 블루프린트 활성화

1. https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 계정 자격 증명으로 로그인합니다.
2. View domain (도메인 보기) 를 선택하고 하나 이상의 빌트인 블루프린트를 활성화하려는 도메인을 선택합니다.
3. 도메인 세부정보 페이지에서 블루프린트 탭으로 이동합니다.
4. 블루프린트 목록에서, DefaultDataLake또는 Amazon SageMaker 블루프린트를 DefaultDataWarehouse선택합니다.
5. 선택한 블루프린트의 세부 정보 페이지에서 이 계정에서 활성화를 선택합니다.
6. 권한 및 리소스 페이지에서 다음을 지정합니다.

   - DefaultDataLake블루프린트를 활성화하는 경우 Glue Manage Access 역할에 대해 DataZone Amazon에 Glue and AWS Lake Formation의 테이블에 대한 액세스를 수집하고 관리할 권한을 부여하는 새 서비스 역할 또는 기존 서비스 역할을 AWS 지정하십시오.
   - DefaultDataWarehouse블루프린트를 활성화하는 경우 Redshift 액세스 관리 역할의 경우 DataZone Amazon Redshift의 데이터 공유, 테이블 및 뷰에 대한 액세스를 수집하고 관리할 권한을 Amazon에 부여하는 신규 또는 기존 서비스 역할을 지정하십시오.
   - Amazon SageMaker 블루프린트를 활성화하는 경우 액세스 SageMaker 관리 역할에 Amazon SageMaker 데이터를 카탈로그에 게시할 DataZone 권한을 Amazon에 부여하는 새 서비스 역할 또는 기존 서비스 역할을 지정하십시오. 또한 Amazon에 카탈로그에 SageMaker 게시된 자산에

대한 액세스 DataZone 권한을 부여하거나 액세스 권한을 취소할 수 있는 권한을 Amazon에 부여합니다.

> **Important**
>
> Amazon SageMaker 블루프린트를 활성화하면 Amazon은 Amazon에 대한 다음 IAM 역할이 현재 계정 및 지역에 DataZone 존재하는지 DataZone 확인합니다. 이러한 역할이 없는 경우 Amazon은 DataZone 해당 역할을 자동으로 생성합니다.
>
> - AmazonDataZoneGlueAccess- <region>- <domainId>
> - AmazonDataZoneRedshiftAccess- <region>- <domainId>

- 프로비저닝 역할의 경우, 환경 계정 및 지역에서 환경 리소스를 생성하고 구성할 수 있는 DataZone 권한을 AWS CloudFormation Amazon에 부여하는 신규 또는 기존 서비스 역할을 지정합니다.
- Amazon SageMaker 블루프린트를 활성화하는 경우 SageMaker-Glue 데이터 소스용 Amazon S3 버킷에 대해 계정의 모든 SageMaker 환경에서 사용할 Amazon S3 버킷을 지정하십시오. AWS 지정하는 버킷 접두사는 다음 중 하나여야 합니다.
  - 아마존-데이터존*
  - 데이터존 세이지메이커*
  - 세이지메이커 - 데이터존*
  - DataZone- 세이지메이커*
  - 세이지메이커- * DataZone
  - DataZone-SageMaker*
  - SageMaker-DataZone*

7. 블루프린트 활성화를 선택합니다.

선택한 블루프린트를 활성화하면 계정의 블루프린트를 사용하여 환경 프로필을 생성할 수 있는 프로젝트를 제어할 수 있습니다. 블루프린트 구성에 관리 프로젝트를 할당하여 이 작업을 수행할 수 있습니다.

활성화된 블루프린트에서 프로젝트 관리를 지정하세요.

1. https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 계정 자격 증명으로 로그인합니다.

2. View Domains를 선택한 다음 선택한 블루프린트에 대한 관리 프로젝트를 추가할 도메인을 선택합니다.
3. 블루프린트 탭을 선택한 다음 작업하려는 블루프린트를 선택합니다.
4. 기본적으로 도메인 내의 모든 프로젝트는 계정의 DefaultDataLake or 또는 또는 DefaultDataWareshouse Amazon SageMaker 블루프린트를 사용하여 환경 프로필을 생성할 수 있습니다. 하지만 블루프린트에 관리 프로젝트를 할당하여 이를 제한할 수 있습니다. 관리 프로젝트를 추가하려면 관리 프로젝트 선택을 선택한 다음 드롭다운 메뉴에서 관리 프로젝트로 추가할 프로젝트를 선택한 다음 관리 프로젝트 선택을 선택합니다.

AWS 계정에서 DefaultDataWarehouse 블루프린트를 활성화하고 나면 블루프린트 구성에 파라미터 세트를 추가할 수 있습니다. 파라미터 세트는 Amazon이 Amazon DataZone Redshift 클러스터에 연결하는 데 필요한 키와 값의 그룹이며 데이터 웨어하우스 환경을 생성하는 데 사용됩니다. 이러한 파라미터에는 Amazon Redshift 클러스터의 이름, 데이터베이스, 클러스터에 대한 자격 증명을 보관하는 AWS 암호가 포함됩니다.

블루프린트에 파라미터 세트 추가 DefaultDataWarehouse

1. https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 계정 자격 증명으로 로그인합니다.
2. View domain (도메인 보기) 를 선택한 다음 파라미터 세트를 추가할 도메인을 선택합니다.
3. 블루프린트 탭을 선택한 다음 블루프린트를 선택하여 DefaultDataWareshouse 블루프린트 세부 정보 페이지를 엽니다.
4. 블루프린트 디테일 페이지의 파라미터 세트 탭에서 파라미터 세트 생성을 선택합니다.
   - 파라미터 세트의 이름을 입력합니다.
   - 파라미터 세트에 대한 설명을 제공할 수도 있습니다.
   - 리전 선택
   - Amazon Redshift 클러스터 또는 Amazon Redshift 서버리스를 선택합니다.
   - 선택한 Amazon Redshift 클러스터 또는 Amazon Redshift 서버리스 워크그룹에 대한 자격 증명이 들어 있는 AWS 보안 ARN을 선택합니다. 파라미터 세트 내에서 사용할 수 있으려면 AWS 암호에 `AmazonDataZoneDomain : [Domain_ID]` 태그 태그를 지정해야 합니다.
     - 기존 AWS 암호가 없는 경우 새 암호 만들기를 선택하여 새 암호를 만들 수도 있습니다. AWS 그러면 암호 이름, 사용자 이름 및 암호를 제공할 수 있는 대화 상자가 열립니다. [Create New AWS Secret] 을 선택하면 Amazon은 AWS Secrets Manager 서비스에 새 비밀번호를

DataZone 생성하고 파라미터 세트를 생성하려는 도메인으로 비밀에 태그가 지정되도록 합니다.

- 위 단계에서 Amazon Redshift 클러스터를 선택했다면 이제 드롭다운에서 클러스터를 선택하십시오. 위 단계에서 Amazon Redshift 워크그룹을 선택했다면 이제 드롭다운에서 워크그룹을 선택하십시오.
- 선택한 Amazon Redshift 클러스터 또는 Amazon Redshift 서버리스 워크그룹 내의 데이터베이스 이름을 입력합니다.
- 파라미터 세트 생성을 선택합니다.

AWS 계정에서 Amazon SageMaker 블루프린트를 활성화하면 블루프린트 구성에 파라미터 세트를 추가할 수 있습니다. 파라미터 세트는 Amazon이 DataZone Amazon에 연결하는 데 필요한 키와 값의 SageMaker 그룹이며, 이를 통해 세이지메이커 환경을 만들 수 있습니다.

Amazon SageMaker 블루프린트에 파라미터 세트 추가

1. https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 계정 자격 증명으로 로그인합니다.
2. View domain (도메인 보기) 를 선택한 다음 파라미터 세트를 추가할 활성화된 블루프린트가 들어 있는 도메인을 선택합니다.
3. Blueprints 탭을 선택한 다음 Amazon SageMaker 청사진을 선택하여 청사진의 세부 정보 페이지를 엽니다.
4. 블루프린트 세부 정보 페이지의 파라미터 세트 탭에서 파라미터 세트 생성을 선택하고 다음을 지정합니다.

   - 파라미터 세트의 이름을 입력합니다.
   - 파라미터 세트에 대한 설명을 제공할 수도 있습니다.
   - Amazon SageMaker 도메인 인증 유형을 지정합니다. IAM 또는 IAM ID 센터 (SSO) 를 선택할 수 있습니다.
   - 지역을 지정하십시오. AWS
   - 데이터 암호화를 위한 AWS KMS 키를 지정합니다. 기존 키를 선택하거나 새 키를 생성할 수 있습니다.
   - 환경 매개변수에서 다음을 지정합니다.
     - VPC ID - 아마존 환경의 VPC에 사용하는 ID입니다. SageMaker 기존 VPC를 지정하거나 새 VPC를 만들 수 있습니다.
     - 서브넷 - VPC 내 특정 리소스의 IP 주소 범위에 대한 하나 이상의 ID.

- 네트워크 액세스 - VPC 전용 또는 공용 인터넷 전용을 선택합니다.
- 보안 그룹 - VPC와 서브넷을 구성할 때 사용할 보안 그룹입니다.

- 데이터 소스 파라미터에서 다음 중 하나를 선택합니다.
  - AWS Glue 전용
  - AWS Glue + 아마존 Redshift 서버리스. 이 옵션을 선택하는 경우 다음을 지정하십시오.
    - 선택한 Amazon Redshift 클러스터의 자격 증명을 보관하는 AWS 보안 ARN을 지정합니다. 파라미터 세트 내에서 사용할 수 있으려면 AWS 암호에 `AmazonDataZoneDomain : [Domain_ID]` 태그 태그를 지정해야 합니다.

      기존 AWS 암호가 없는 경우 새 암호 만들기를 선택하여 새 암호를 만들 수도 있습니다. AWS 그러면 암호 이름, 사용자 이름 및 암호를 제공할 수 있는 대화 상자가 열립니다. [Create New AWS Secret] 을 선택하면 Amazon은 AWS Secrets Manager 서비스에 새 비밀번호를 DataZone 생성하고 파라미터 세트를 생성하려는 도메인으로 비밀에 태그가 지정되도록 합니다.
    - 환경을 생성할 때 사용할 Amazon Redshift 워크그룹을 지정하십시오.
    - 환경을 생성할 때 사용하려는 데이터베이스 (선택한 작업 그룹 내) 의 이름을 지정합니다.
  - AWS Glue only + 아마존 Redshift 클러스터
    - 선택한 Amazon Redshift 클러스터의 자격 증명을 보관하는 AWS 보안 ARN을 지정합니다. 파라미터 세트 내에서 사용할 수 있으려면 AWS 암호에 `AmazonDataZoneDomain : [Domain_ID]` 태그 태그를 지정해야 합니다.

      기존 AWS 암호가 없는 경우 새 암호 만들기를 선택하여 새 암호를 만들 수도 있습니다. AWS 그러면 암호 이름, 사용자 이름 및 암호를 제공할 수 있는 대화 상자가 열립니다. [Create New AWS Secret] 을 선택하면 Amazon은 AWS Secrets Manager 서비스에 새 비밀번호를 DataZone 생성하고 파라미터 세트를 생성하려는 도메인으로 비밀에 태그가 지정되도록 합니다.
    - 환경을 생성할 때 사용하려는 Amazon Redshift 클러스터를 지정하십시오.
    - 환경을 만들 때 사용하려는 데이터베이스 (선택한 클러스터 내) 의 이름을 지정합니다.

5. 파라미터 세트 생성을 선택합니다.

Amazon SageMaker 도메인을 소유한 AWS 계정에서 DataZone Amazon을 신뢰할 수 있는 서비스로 추가

Amazon SageMaker 블루프린트를 활성화한 경우 Amazon DataZone 내에 신뢰할 수 있는 서비스 중 SageMaker 하나로 추가해야 합니다. 이렇게 하려면 다음 절차를 완료하십시오.

1. https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 계정 자격 증명으로 로그인합니다.
2. View domain (도메인 보기) 를 선택한 다음 활성화된 SageMaker 블루프린트가 들어 있는 도메인을 선택합니다.
3. 신뢰할 수 있는 서비스를 선택한 다음 SageMakerAmazon을 선택한 다음 활성화를 선택합니다.

관련 계정을 사용하여 데이터 게시 및 사용

AWS 계정을 Amazon DataZone 도메인과 연결하면 도메인 사용자가 해당 계정의 데이터를 게시하고 사용할 수 있습니다. AWS 계정 연결을 설정하는 데는 세 단계가 있습니다.

- 먼저 연결을 요청하여 원하는 AWS 계정과 도메인을 공유하세요. DataZone Amazon은 계정이 도메인 AWS 계정과 다른 경우 AWS Resource Access Manager (RAM) 를 사용합니다. AWS 계정 연결은 Amazon DataZone 도메인에서만 시작할 수 있습니다.
- 둘째, 계정 소유자가 연결 요청을 수락하도록 하십시오.
- 셋째, 계정 소유자가 원하는 환경 블루프린트를 활성화하도록 하세요. 블루프린트를 활성화함으로써 계정 소유자는 도메인의 사용자에게 자신의 계정에서 AWS Glue 데이터베이스 및 Amazon Redshift 클러스터와 같은 리소스를 생성하고 액세스하는 데 필요한 IAM 역할 및 리소스 구성을 제공합니다.

주제

다른 계정과의 연결 요청 AWS

> **Note**
>
> 다른 AWS 계정으로 연결 요청을 보내면 AWS Resource Access Manager (RAM) 를 통해 다른 AWS 계정과 도메인을 공유하는 것입니다. 입력한 계정 ID가 정확한지 확인하세요.

Amazon DataZone 콘솔에서 Amazon DataZone 도메인의 다른 AWS 계정과의 연결을 요청하려면 관리자 권한이 있는 계정에서 IAM 역할을 수임해야 합니다. Amazon DataZone 관리 콘솔을 사용하는 데 필요한 IAM 권한을 구성합니다.계정 연결을 요청하는 데 필요한 최소 권한을 얻으려면

다른 AWS 계정과의 연결을 요청하려면 다음 절차를 완료하십시오.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 관리 콘솔을 엽니다.
2. 도메인 보기를 선택하고 목록에서 도메인 이름을 선택합니다. 이름은 하이퍼링크입니다.
3. 아래로 스크롤하여 관련 계정 탭으로 이동한 다음 연결 요청을 선택합니다.
4. 연결을 요청하려는 계정의 ID를 입력합니다. 계정 ID 목록에 만족하면 연결 요청을 선택합니다.
5. Amazon은 사용자 계정을 대신하여 AWS Resource Access Manager에서 입력한 계정 ID를 보안 주체로 사용하여 리소스 공유를 DataZone 생성합니다.
6. 요청을 수락하려면 다른 AWS 계정의 소유자에게 알려야 합니다. 초대는 7일 후에 만료됩니다.

고객 관리형 KMS 키에 대한 계정 액세스 권한을 제공하십시오.

Amazon DataZone 도메인과 메타데이터는 기본적으로 AWS보유한 키를 사용하거나 (선택 사항) 도메인 생성 중에 사용자가 소유하고 제공하는 KMS (Key Management Service) 의 고객 관리 AWS 키를 사용하여 암호화됩니다. 도메인이 고객 관리형 키로 암호화된 경우 아래 절차에 따라 관련 계정에 KMS 키를 사용할 권한을 부여하십시오.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/kms/ 에서 KMS 콘솔을 엽니다.
2. 해당 계정에서 직접 생성하고 관리하는 키를 보려면 탐색 창에서 고객 관리형 키를 선택합니다.
3. 해당 계정에서 직접 생성하고 관리하는 키를 보려면 탐색 창에서 고객 관리형 키를 선택합니다.
4. KMS 키 목록에서 검사하려는 KMS 키의 별칭 또는 키 ID를 선택합니다.
5. 외부 AWS 계정의 KMS 키 사용을 허용하거나 허용하지 않으려면 페이지의 기타 AWS 계정 섹션에 있는 컨트롤을 사용하십시오. 적절한 KMS 권한이 있는 이러한 계정의 IAM 보안 주체는 암호화, 암호 해독, 재암호화 및 데이터 키 생성과 같은 암호화 작업에 KMS 키를 사용할 수 있습니다.

Amazon DataZone 도메인의 계정 연결 요청을 수락하고 환경 블루프린트를 활성화합니다.

Amazon DataZone 관리 콘솔에서 Amazon DataZone 도메인과 연결을 허용하려면 관리자 권한이 있는 계정에서 IAM 역할을 수임해야 합니다. Amazon DataZone 관리 콘솔을 사용하는 데 필요한 IAM 권한을 구성합니다.최소 권한을 얻으려면

Amazon DataZone 도메인과의 연결을 수락하려면 다음을 완료하십시오.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 관리 콘솔을 엽니다.
2. 요청 보기를 선택하고 목록에서 초대 도메인을 선택합니다. 초대 상태를 요청해야 합니다. 검토 요청을 선택합니다.
3. 상자를 둘 다 선택하거나 둘 다 선택하거나 둘 중 하나를 선택하여 기본 데이터 레이크 및/또는 데이터 웨어하우스 환경 블루프린트를 활성화할지 여부를 선택합니다. 나중에 이 작업을 수행할 수 있습니다.

   - 데이터 레이크 환경 청사진을 사용하면 도메인 사용자가 AWS Glue, Amazon S3 및 Amazon Athena 리소스를 생성하고 관리하여 데이터 레이크에서 게시하고 사용할 수 있습니다.
   - 데이터 웨어하우스 환경 청사진을 사용하면 도메인 사용자가 Amazon Redshift 리소스를 생성 및 관리하여 데이터 웨어하우스에서 게시하고 사용할 수 있습니다.
4. 기본 환경 청사진 중 하나 또는 둘 다를 선택하는 경우 다음 권한과 리소스를 구성하십시오.

   - 액세스 관리 IAM 역할은 도메인 사용자가 AWS Glue 및 Amazon DataZone Redshift와 같은 테이블에 대한 액세스를 수집하고 관리할 수 있는 권한을 Amazon에 제공합니다. Amazon에서 새 IAM 역할을 DataZone 생성하여 사용하도록 하거나 기존 IAM 역할 목록에서 선택할 수 있습니다.
   - 프로비저닝 IAM 역할은 도메인 사용자가 AWS Glue 데이터베이스와 같은 환경 리소스를 생성하고 구성할 수 있는 권한을 DataZone Amazon에 제공합니다. Amazon에서 새 IAM 역할을 DataZone 생성하여 사용하도록 하거나 기존 IAM 역할 목록에서 선택할 수 있습니다.
   - Data Lake용 Amazon S3 버킷은 도메인 사용자가 데이터 레이크 데이터를 저장할 때 DataZone Amazon이 사용하는 버킷 또는 경로입니다. Amazon에서 선택한 기본 버킷을 DataZone 사용하거나 경로 문자열을 입력하여 기존 Amazon S3 경로를 직접 선택할 수 있습니다. Amazon S3 경로를 직접 선택하는 경우 Amazon에 사용 권한을 제공하도록 IAM 정책을 업데이트해야 합니다. DataZone
5. 구성이 만족스러우면 수락을 선택하고 연결을 구성합니다.

Amazon DataZone 도메인의 계정 연결 요청 거부

Amazon DataZone 관리 콘솔에서 Amazon DataZone 도메인의 연결 요청을 거부하려면 관리자 권한이 있는 계정에서 IAM 역할을 수임해야 합니다. Amazon DataZone 관리 콘솔을 사용하는 데 필요한 IAM 권한을 구성합니다.최소 권한을 얻으려면

Amazon DataZone 도메인의 연결 요청을 거부하려면 다음을 완료하십시오.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 관리 콘솔을 엽니다.
2. 요청 보기를 선택하고 목록에서 초대 도메인을 선택합니다. 초대 상태를 요청해야 합니다. 연결 거부를 선택합니다. 연결 거부를 선택하여 선택을 확인합니다.

관련 계정에서 환경 블루프린트를 활성화하세요. AWS

Amazon DataZone 관리 콘솔에서 환경 블루프린트를 활성화하려면 관리자 권한이 있는 계정에서 IAM 역할을 수임해야 합니다. Amazon DataZone 관리 콘솔을 사용하는 데 필요한 IAM 권한을 구성합니다.최소 권한을 얻으려면

관련 도메인에서 블루프린트를 활성화하려면 다음을 완료하세요.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 관리 콘솔을 엽니다.
2. 왼쪽 탐색 패널을 열고 관련 도메인을 선택합니다.
3. 환경 블루프린트를 활성화하려는 도메인을 선택합니다.
4. 블루프린트 목록에서, DefaultDataLake또는 Amazon SageMaker 블루프린트를 DefaultDataWarehouse선택합니다.
5. 선택한 블루프린트의 세부 정보 페이지에서 이 계정에서 활성화를 선택합니다.
6. 권한 및 리소스 페이지에서 다음을 지정합니다.

   - DefaultDataLake블루프린트를 활성화하는 경우 Glue Manage Access 역할에 대해 DataZone Amazon에 Glue and AWS Lake Formation의 테이블을 수집하고 이에 대한 액세스를 관리할 권한을 부여하는 신규 또는 기존 서비스 역할을 AWS 지정하십시오.
   - DefaultDataWarehouse블루프린트를 활성화하는 경우 Redshift 액세스 관리 역할의 경우 DataZone Amazon Redshift의 데이터 공유, 테이블 및 뷰에 대한 액세스를 수집하고 관리할 권한을 Amazon에 부여하는 신규 또는 기존 서비스 역할을 지정하십시오.
   - Amazon SageMaker 블루프린트를 활성화하는 경우 액세스 SageMaker 관리 역할에 Amazon SageMaker 데이터를 카탈로그에 게시할 DataZone 권한을 Amazon에 부여하는 새 서비스 역할 또는 기존 서비스 역할을 지정하십시오. 또한 Amazon에 카탈로그에 SageMaker 게시된 자산에 대한 액세스 DataZone 권한을 부여하거나 액세스 권한을 취소할 수 있는 권한을 Amazon에 부여합니다.

> **Important**
>
> Amazon SageMaker 블루프린트를 활성화하면 Amazon은 Amazon의 다음 IAM 역할이 현재 계정 및 지역에 DataZone 존재하는지 DataZone 확인합니다. 이러한 역할이 없는 경우 Amazon은 DataZone 해당 역할을 자동으로 생성합니다.
>
> - AmazonDataZoneGlueAccess- <region>- <domainId>
> - AmazonDataZoneRedshiftAccess- <region>- <domainId>

- 프로비저닝 역할의 경우, 환경 계정 및 지역에서 환경 리소스를 생성하고 구성할 수 있는 DataZone 권한을 Amazon에 부여하는 새 서비스 역할 또는 기존 서비스 역할을 지정합니다. AWS CloudFormation
- Amazon SageMaker 블루프린트를 활성화하는 경우 SageMaker-Glue 데이터 소스용 Amazon S3 버킷에 대해 계정의 모든 SageMaker 환경에서 사용할 Amazon S3 버킷을 지정하십시오. AWS 지정하는 버킷 접두사는 다음 중 하나여야 합니다.
  - 아마존-데이터존*
  - 데이터존 세이지메이커*
  - 세이지메이커 - 데이터존*
  - DataZone- 세이지메이커*
  - 세이지메이커- * DataZone
  - DataZone-SageMaker*
  - SageMaker-DataZone*

7. 블루프린트 활성화를 선택합니다.

선택한 블루프린트를 활성화하면 계정의 블루프린트를 사용하여 환경 프로필을 생성할 수 있는 프로젝트를 제어할 수 있습니다. 블루프린트 구성에 관리 프로젝트를 할당하여 이 작업을 수행할 수 있습니다.

활성화된 DefaultDataLake 프로젝트 또는 블루프린트에서 프로젝트 관리를 지정하십시오. DefaultDataWarehouse

1. https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 계정 자격 증명으로 로그인합니다.
2. 왼쪽 탐색 패널을 열고 관련 도메인을 선택한 다음 관리 프로젝트를 추가할 도메인을 선택합니다.

3. 블루프린트 탭을 선택한 다음 DefaultDataLake 또는 DefaultDataWareshouse 블루프린트를 선택합니다.
4. 기본적으로 도메인 내 모든 프로젝트는 계정의 DefaultDataLake 또는 DefaultDataWareshouse 블루프린트를 사용하여 환경 프로필을 만들 수 있습니다. 하지만 블루프린트에 관리 프로젝트를 할당하여 이를 제한할 수 있습니다. 관리 프로젝트를 추가하려면 관리 프로젝트 선택을 선택한 다음 드롭다운 메뉴에서 관리 프로젝트로 추가할 프로젝트를 선택한 다음 관리 프로젝트 선택을 선택합니다.

AWS 계정에서 DefaultDataWarehouse 블루프린트를 활성화하고 나면 블루프린트 구성에 파라미터 세트를 추가할 수 있습니다. 파라미터 세트는 Amazon이 Amazon DataZone Redshift 클러스터에 연결하는 데 필요한 키와 값의 그룹이며 데이터 웨어하우스 환경을 생성하는 데 사용됩니다. 이러한 파라미터에는 Amazon Redshift 클러스터의 이름, 데이터베이스, 클러스터에 대한 자격 증명을 보관하는 AWS 암호가 포함됩니다.

블루프린트에 파라미터 세트 추가 DefaultDataWarehouse

1. https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 계정 자격 증명으로 로그인합니다.
2. 왼쪽 탐색 패널을 열고 Associated domain (Associated domain) 을 선택한 다음 파라미터 세트를 추가할 도메인을 선택합니다.
3. 블루프린트 탭을 선택한 다음 블루프린트를 선택하여 DefaultDataWareshouse 블루프린트 세부 정보 페이지를 엽니다.
4. 블루프린트 디테일 페이지의 파라미터 세트 탭에서 파라미터 세트 생성을 선택합니다.
   - 파라미터 세트의 이름을 입력합니다.
   - 파라미터 세트에 대한 설명을 제공할 수도 있습니다.
   - 리전 선택
   - Amazon Redshift 클러스터 또는 Amazon Redshift 서버리스를 선택합니다.
   - 선택한 Amazon Redshift 클러스터 또는 Amazon Redshift 서버리스 워크그룹에 대한 자격 증명이 들어 있는 AWS 보안 ARN을 선택합니다. 파라미터 세트 내에서 사용할 수 있으려면 AWS 암호에 `AmazonDataZoneDomain : [Domain_ID]` 태그 태그를 지정해야 합니다.
     - 기존 AWS 암호가 없는 경우 새 암호 만들기를 선택하여 새 암호를 만들 수도 있습니다. AWS 그러면 암호 이름, 사용자 이름 및 암호를 제공할 수 있는 대화 상자가 열립니다. [Create New AWS Secret] 을 선택하면 Amazon은 AWS Secrets Manager 서비스에 새 비밀번호를

DataZone 생성하고 파라미터 세트를 생성하려는 도메인으로 비밀에 태그가 지정되도록 합니다.

- Amazon Redshift 클러스터 또는 Amazon Redshift 서버리스 워크그룹을 선택합니다.
- 선택한 Amazon Redshift 클러스터 또는 Amazon Redshift 서버리스 워크그룹 내의 데이터베이스 이름을 입력합니다.
- 파라미터 세트 생성을 선택합니다.

AWS 계정에서 Amazon SageMaker 블루프린트를 활성화하면 블루프린트 구성에 파라미터 세트를 추가할 수 있습니다. 파라미터 세트는 Amazon이 DataZone Amazon에 연결하는 데 필요한 키와 값의 SageMaker 그룹이며, 이를 통해 세이지메이커 환경을 만들 수 있습니다.

Amazon SageMaker 블루프린트에 파라미터 세트 추가

1. https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 계정 자격 증명으로 로그인합니다.
2. View domain (도메인 보기) 를 선택한 다음 파라미터 세트를 추가할 활성화된 블루프린트가 들어 있는 도메인을 선택합니다.
3. Blueprints 탭을 선택한 다음 Amazon SageMaker 청사진을 선택하여 청사진의 세부 정보 페이지를 엽니다.
4. 블루프린트 세부 정보 페이지의 파라미터 세트 탭에서 파라미터 세트 생성을 선택하고 다음을 지정합니다.

   - 파라미터 세트의 이름을 입력합니다.
   - 파라미터 세트에 대한 설명을 제공할 수도 있습니다.
   - Amazon SageMaker 도메인 인증 유형을 지정합니다. IAM 또는 IAM ID 센터 (SSO) 를 선택할 수 있습니다.
   - 지역을 지정합니다. AWS
   - 데이터 암호화를 위한 AWS KMS 키를 지정합니다. 기존 키를 선택하거나 새 키를 생성할 수 있습니다.
   - 환경 매개변수에서 다음을 지정합니다.
     - VPC ID - 아마존 환경의 VPC에 사용하는 ID입니다. SageMaker 기존 VPC를 지정하거나 새 VPC를 만들 수 있습니다.
     - 서브넷 - VPC 내 특정 리소스의 IP 주소 범위에 대한 하나 이상의 ID.
     - 네트워크 액세스 - VPC 전용 또는 공용 인터넷 전용을 선택합니다.

- 보안 그룹 - VPC와 서브넷을 구성할 때 사용할 보안 그룹.

- 데이터 소스 파라미터에서 다음 중 하나를 선택합니다.
  - AWS Glue 전용
  - AWS Glue + 아마존 Redshift 서버리스. 이 옵션을 선택하는 경우 다음을 지정하십시오.
    - 선택한 Amazon Redshift 클러스터의 자격 증명을 보관하는 AWS 보안 ARN을 지정합니다. 파라미터 세트 내에서 사용할 수 있으려면 AWS 암호에 `AmazonDataZoneDomain : [Domain_ID]` 태그 태그를 지정해야 합니다.

      기존 AWS 암호가 없는 경우 새 암호 만들기를 선택하여 새 암호를 만들 수도 있습니다. AWS 그러면 암호 이름, 사용자 이름 및 암호를 제공할 수 있는 대화 상자가 열립니다. [Create New AWS Secret] 을 선택하면 Amazon은 AWS Secrets Manager 서비스에 새 비밀번호를 DataZone 생성하고 파라미터 세트를 생성하려는 도메인으로 비밀에 태그가 지정되도록 합니다.
    - 환경을 생성할 때 사용할 Amazon Redshift 워크그룹을 지정하십시오.
    - 환경을 생성할 때 사용하려는 데이터베이스 (선택한 작업 그룹 내) 의 이름을 지정합니다.
  - AWS Glue only + 아마존 Redshift 클러스터
    - 선택한 Amazon Redshift 클러스터의 자격 증명을 보관하는 AWS 보안 ARN을 지정합니다. 파라미터 세트 내에서 사용할 수 있으려면 AWS 암호에 `AmazonDataZoneDomain : [Domain_ID]` 태그 태그를 지정해야 합니다.

      기존 AWS 암호가 없는 경우 새 암호 만들기를 선택하여 새 암호를 만들 수도 있습니다. AWS 그러면 암호 이름, 사용자 이름 및 암호를 제공할 수 있는 대화 상자가 열립니다. [Create New AWS Secret] 을 선택하면 Amazon은 AWS Secrets Manager 서비스에 새 비밀번호를 DataZone 생성하고 파라미터 세트를 생성하려는 도메인으로 비밀에 태그가 지정되도록 합니다.
    - 환경을 생성할 때 사용하려는 Amazon Redshift 클러스터를 지정하십시오.
    - 환경을 생성할 때 사용하려는 데이터베이스 (선택한 클러스터 내) 의 이름을 지정합니다.

5. 파라미터 세트 생성을 선택합니다.

관련 AWS 계정에서 SageMaker Amazon을 신뢰할 수 있는 서비스로 추가

Amazon SageMaker 블루프린트를 활성화한 경우 Amazon DataZone 내에 신뢰할 수 있는 서비스 중 SageMaker 하나로 추가해야 합니다. 이렇게 하려면 다음 절차를 완료하십시오.

1. https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 계정 자격 증명으로 로그인합니다.
2. View domain (도메인 보기) 를 선택한 다음 활성화된 SageMaker 블루프린트가 들어 있는 도메인을 선택합니다.
3. 신뢰할 수 있는 서비스를 선택한 다음 SageMakerAmazon을 선택한 다음 활성화를 선택합니다.

관련 계정 제거

Amazon DataZone 관리 콘솔에서 관련 AWS 계정을 제거하려면 관리자 권한이 있는 계정에서 IAM 역할을 수임해야 합니다. Amazon DataZone 관리 콘솔을 사용하는 데 필요한 IAM 권한을 구성합니다.최소 권한을 얻으려면

도메인에서 관련 계정을 제거하려면 다음 절차를 완료하세요.

1. AWS 관리 콘솔에 로그인하고 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 관리 콘솔을 엽니다.
2. [도메인 보기] 를 선택하고 목록에서 도메인 이름을 선택합니다. 이름은 하이퍼링크입니다.
3. 아래로 스크롤하여 관련 계정 탭으로 이동합니다. 제거하려는 계정의 AWS 계정 ID를 선택합니다.
4. 연결 해제를 선택합니다. 필드에 연결 해제를 입력하고 연결 해제를 선택하여 선택을 확인합니다.
5. 이제 도메인에서 계정이 제거되었으며 도메인 사용자는 해당 계정을 사용하여 데이터를 게시하고 사용할 수 없습니다.

Amazon DataZone 데이터 카탈로그 사용

Amazon DataZone 비즈니스 데이터 카탈로그를 사용하여 비즈니스 컨텍스트와 함께 조직 전체의 데이터를 카탈로그화하여 조직의 모든 사람이 데이터를 빠르게 찾고 이해할 수 있도록 할 수 있습니다. 자세한 정보는 아마존 DataZone 용어 및 개념을 참조하세요.

주제

비즈니스 용어집 생성, 편집 또는 삭제

DataZoneAmazon에서 비즈니스 용어집은 자산 (데이터) 과 연관될 수 있는 비즈니스 용어 (단어) 의 모음입니다. 비즈니스 사용자가 데이터를 분석할 때 조직 전체에서 동일한 정의를 사용할 수 있도록 비즈니스 용어 및 정의 목록과 함께 적절한 어휘를 제공합니다. 비즈니스 용어집은 카탈로그 도메인에서 생성되며 자산 및 열에 적용하여 해당 자산 또는 열의 주요 특성을 이해하는 데 도움이 될 수 있습니다. 하나 이상의 용어집 용어를 적용할 수 있습니다. 비즈니스 용어집은 비즈니스 용어집의 모든 용어를 다른 용어의 하위 목록과 연결할 수 있는 간단한 용어 목록일 수 있습니다. 자세한 정보는 아마존 DataZone 용어 및 개념을 참조하세요. Amazon DataZone 도메인에서 용어집을 생성, 편집 또는 삭제하려면 해당 도메인에 대한 적절한 권한을 가진 소유 프로젝트의 구성원이어야 합니다.

용어집을 만들려면 다음 단계를 완료하세요.

1. 데이터 포털 URL을 사용하여 Amazon DataZone 데이터 포털로 이동하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생성된 AWS 계정의 Amazon DataZone 콘솔에서 https://console.aws.amazon.com/datazone 에 액세스하여 데이터 포털 URL을 확인할 수 있습니다.
2. 검색 옆의 상단 탐색 표시줄에서 카탈로그 메뉴로 이동합니다.
3. Amazon DataZone Data Portal에서 용어집을 선택한 다음 용어집 생성을 선택합니다.
4. 용어집의 이름, 설명, 소유자를 지정한 다음 용어집 생성을 선택합니다.
5. 활성화 토글을 선택하여 새 용어집을 활성화합니다.
6. 용어집의 세부정보 페이지에서 Readme 생성을 선택하여 이 용어집에 대한 몇 가지 추가 정보를 추가할 수 있습니다.

비즈니스 용어집을 비활성화하거나 활성화하려면 다음 단계를 완료하세요.

1. 데이터 포털 URL을 사용하여 Amazon DataZone 데이터 포털로 이동하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생성된 AWS 계정의 Amazon DataZone 콘솔에서 https://console.aws.amazon.com/datazone 에 액세스하여 데이터 포털 URL을 확인할 수 있습니다.
2. 검색 옆의 상단 탐색 표시줄에서 카탈로그 메뉴로 이동합니다.
3. Amazon DataZone Data Portal에서 용어집을 선택하고 비활성화/활성화하려는 비즈니스 용어집을 찾습니다.
4. 용어집 세부 정보 페이지에서 활성화/비활성화 토글을 찾아 선택한 용어집을 활성화 또는 비활성화하는 데 사용합니다.

> **Note**
>
> 용어집을 비활성화하면 해당 용어집에 포함된 모든 용어도 비활성화됩니다.

비즈니스 용어집을 편집하려면 다음 단계를 완료하세요.

1. 데이터 포털 URL을 사용하여 Amazon DataZone 데이터 포털로 이동하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생성된 AWS 계정의 Amazon DataZone 콘솔에서 https://console.aws.amazon.com/datazone 에 액세스하여 데이터 포털 URL을 확인할 수 있습니다.
2. 검색 옆의 상단 탐색 표시줄에서 카탈로그 메뉴로 이동합니다.
3. Amazon DataZone Data Portal에서 용어집을 선택하고 편집하려는 비즈니스 용어집을 찾습니다.
4. 용어집 세부 정보 페이지에서 작업을 확장한 다음 편집을 선택하여 용어집을 편집합니다.
5. 이름, 설명을 업데이트한 다음 [Save] 를 선택합니다.

비즈니스 용어집을 삭제하려면 다음 단계를 완료하세요.

1. 데이터 포털 URL을 사용하여 Amazon DataZone 데이터 포털로 이동하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생성된 AWS 계정의 Amazon DataZone 콘솔에서 https://console.aws.amazon.com/datazone 에 액세스하여 데이터 포털 URL을 확인할 수 있습니다.
2. 검색 옆의 상단 탐색 표시줄에서 카탈로그 메뉴로 이동합니다.
3. Amazon DataZone Data Portal에서 용어집을 선택하고 삭제하려는 비즈니스 용어집을 찾습니다.

4. 용어집 세부 정보 페이지에서 작업을 확장한 다음 삭제를 선택하여 용어집을 삭제합니다.

> **Note**
>
> 용어집을 삭제하려면 먼저 용어집의 기존 용어를 모두 삭제해야 합니다.

5. 삭제를 선택하여 용어집 삭제를 확인합니다.

용어집에서 용어 생성, 수정 또는 삭제

DataZoneAmazon에서 비즈니스 용어집은 자산 (데이터) 과 연관될 수 있는 비즈니스 용어 모음입니다. 자세한 정보는 아마존 DataZone 용어 및 개념을 참조하세요. Amazon DataZone 도메인에서 용어집의 용어를 생성, 편집 또는 삭제하려면 해당 도메인에 대한 적절한 권한을 가진 소유 프로젝트의 구성원이어야 합니다.

DataZoneAmazon에서는 비즈니스 용어집 용어를 자세히 설명할 수 있습니다. 특정 용어의 컨텍스트를 설정하기 위해 용어 간의 관계를 지정할 수 있습니다. 용어에 대한 관계를 정의하면 관련 용어의 정의에 자동으로 추가됩니다. Amazon에서 사용할 수 있는 용어집 용어 DataZone 관계에는 다음이 포함됩니다.

- 유형 - 현재 용어가 식별된 용어의 유형임을 나타냅니다. 식별된 용어가 현재 용어의 상위 용어임을 나타냅니다.
- 유형 포함 - 현재 용어가 지정된 특정 용어에 대한 일반적인 용어임을 나타냅니다. 이 관계는 일반 용어의 하위 용어를 나타낼 수 있습니다.

새 용어를 만들려면 다음 단계를 완료하세요.

1. 데이터 포털 URL을 사용하여 Amazon DataZone 데이터 포털로 이동하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생성된 AWS 계정의 Amazon DataZone 콘솔에서 https://console.aws.amazon.com/datazone 에 액세스하여 데이터 포털 URL을 확인할 수 있습니다.
2. 검색 옆의 상단 탐색 표시줄에서 카탈로그 메뉴로 이동합니다.
3. Amazon DataZone Data Portal에서 용어집을 선택한 다음 새 용어를 생성할 용어집을 선택합니다.
4. 용어의 이름, 설명, 소유자를 지정한 다음 [Create term] 을 선택합니다.
5. 활성화 토글을 선택하여 새 용어를 활성화합니다.

6. Readme를 추가하려면 용어 세부 정보 페이지로 이동한 다음 Readme 생성을 선택하여 이 용어집에 대한 몇 가지 추가 정보를 추가할 수 있습니다.
7. 관계를 추가하려면 용어 세부 정보 페이지로 이동하여 용어 관계 섹션을 선택한 다음 용어집 용어 추가를 선택합니다. 대화 상자에서 연관시키려는 관계와 용어를 선택한 다음 [닫기] 를 선택하여 적절한 관계 유형에 용어를 추가합니다. 이 관계는 관련 용어로 만든 모든 용어에도 추가됩니다.

용어집에서 용어를 편집하려면 다음 단계를 완료하십시오.

1. 데이터 포털 URL을 사용하여 Amazon DataZone 데이터 포털로 이동하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생성된 AWS 계정의 Amazon DataZone 콘솔에서 https://console.aws.amazon.com/datazone 에 액세스하여 데이터 포털 URL을 확인할 수 있습니다.
2. 검색 옆의 상단 탐색 표시줄에서 카탈로그 메뉴로 이동합니다.
3. Amazon DataZone Data Portal에서 용어집을 선택하고 편집하려는 용어가 포함된 용어집을 찾은 다음 해당 용어를 선택합니다.
4. 용어 세부 정보 페이지에서 작업을 확장한 다음 편집을 선택하여 용어를 편집합니다.
5. 이름, 설명을 업데이트한 다음 [Save] 를 선택합니다.

용어집에서 용어를 삭제하려면 다음 단계를 완료하세요.

1. 데이터 포털 URL을 사용하여 Amazon DataZone 데이터 포털로 이동하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생성된 AWS 계정의 Amazon DataZone 콘솔에서 https://console.aws.amazon.com/datazone 에 액세스하여 데이터 포털 URL을 확인할 수 있습니다.
2. 검색 옆의 상단 탐색 표시줄에서 카탈로그 메뉴로 이동합니다.
3. Amazon DataZone Data Portal에서 용어집을 선택하고 삭제하려는 용어가 포함된 용어집을 찾은 다음 해당 용어를 선택합니다.
4. 용어집 세부 정보 페이지에서 작업을 확장한 다음 삭제를 선택하여 용어를 삭제합니다.
5. 삭제를 선택하여 용어 삭제를 확인합니다.

메타데이터 양식을 생성, 편집 또는 삭제합니다.

DataZoneAmazon에서 메타데이터 양식은 카탈로그의 자산 메타데이터에 추가 비즈니스 컨텍스트를 보강하기 위한 간단한 양식입니다. 이는 데이터 소유자가 데이터 사용자가 데이터를 검색하고 찾을 때

도움이 될 수 있는 정보로 자산을 보강할 수 있는 확장 가능한 메커니즘 역할을 합니다. 또한 메타데이터 양식은 Amazon DataZone 카탈로그에 게시되는 모든 자산의 일관성을 유지하는 메커니즘을 제공할 수 있습니다.

메타데이터 양식 정의는 부울, 날짜, 십진수, 정수, 문자열 및 비즈니스 용어집 필드 값 데이터 유형을 지원하는 하나 이상의 필드 정의로 구성됩니다. 자세한 정보는 아마존 DataZone 용어 및 개념을 참조하세요. Amazon DataZone 도메인에서 메타데이터 양식을 생성, 편집 또는 삭제하려면 올바른 자격 증명을 가진 소유 프로젝트의 구성원이어야 합니다.

메타데이터 양식을 생성하려면 다음 단계를 완료하십시오.

1. 데이터 포털 URL을 사용하여 Amazon DataZone 데이터 포털로 이동하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생성된 AWS 계정의 Amazon DataZone 콘솔에서 https://console.aws.amazon.com/datazone 에 액세스하여 데이터 포털 URL을 확인할 수 있습니다.
2. 검색 옆의 상단 탐색 표시줄에서 카탈로그 메뉴로 이동합니다.
3. Amazon DataZone Data Portal에서 메타데이터 양식을 선택한 다음 양식 생성을 선택합니다.
4. 메타데이터 양식 이름, 설명, 소유자를 지정한 다음 양식 생성을 선택합니다.

메타데이터 양식을 편집하려면 다음 단계를 완료하세요.

1. 데이터 포털 URL을 사용하여 Amazon DataZone 데이터 포털로 이동하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생성된 AWS 계정의 Amazon DataZone 콘솔에서 https://console.aws.amazon.com/datazone 에 액세스하여 데이터 포털 URL을 확인할 수 있습니다.
2. 검색 옆의 상단 탐색 표시줄에서 카탈로그 메뉴로 이동합니다.
3. Amazon DataZone Data Portal에서 [메타데이터 양식] 을 선택한 다음 편집하려는 메타데이터 양식을 찾습니다.
4. 메타데이터 양식의 세부 정보 페이지에서 작업을 확장한 다음 편집을 선택합니다.
5. 이름, 설명, 소유자 필드를 업데이트한 다음 양식 업데이트를 선택합니다.

메타데이터 양식을 삭제하려면 다음 단계를 완료하세요.

> **Note**
>
> 메타데이터 양식을 삭제하려면 먼저 해당 양식이 적용된 모든 자산 유형 또는 자산에서 해당 양식을 제거해야 합니다.

1. 데이터 포털 URL을 사용하여 Amazon DataZone 데이터 포털로 이동하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생성된 AWS 계정의 Amazon DataZone 콘솔에서 https://console.aws.amazon.com/datazone 에 액세스하여 데이터 포털 URL을 확인할 수 있습니다.
2. 검색 옆의 상단 탐색 표시줄에서 카탈로그 메뉴로 이동합니다.
3. Amazon DataZone Data Portal에서 [메타데이터 양식] 을 선택한 다음 삭제하려는 메타데이터 양식을 찾습니다.
4. 삭제하려는 메타데이터 양식이 활성화된 경우 활성화 토글을 선택하여 메타데이터 양식을 비활성화하십시오.
5. 메타데이터 양식의 세부 정보 페이지에서 작업을 확장한 다음 삭제를 선택합니다.
6. 삭제를 선택하여 삭제를 확인합니다.

메타데이터 양식에서 필드를 생성, 편집 또는 삭제합니다.

DataZoneAmazon에서 메타데이터 양식은 카탈로그의 자산 메타데이터에 추가 비즈니스 컨텍스트를 보강하기 위한 간단한 양식입니다. 이는 데이터 소유자가 데이터 사용자가 데이터를 검색하고 찾을 때 도움이 될 수 있는 정보로 자산을 보강할 수 있는 확장 가능한 메커니즘 역할을 합니다. 또한 메타데이터 양식은 Amazon DataZone 카탈로그에 게시되는 모든 자산의 일관성을 유지하는 메커니즘을 제공할 수 있습니다.

메타데이터 양식 정의는 부울, 날짜, 십진수, 정수, 문자열 및 비즈니스 용어집 필드 값 데이터 유형을 지원하는 하나 이상의 필드 정의로 구성됩니다. 자세한 정보는 아마존 DataZone 용어 및 개념을 참조하세요. Amazon DataZone 도메인의 메타데이터 양식에서 필드를 생성, 편집 또는 삭제하려면 올바른 자격 증명을 가진 소유 프로젝트의 구성원이어야 합니다.

메타데이터 양식에서 필드를 생성하려면 다음 단계를 완료하십시오.

1. 데이터 포털 URL을 사용하여 Amazon DataZone 데이터 포털로 이동하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생성된 AWS 계정의 Amazon DataZone 콘솔에서 https://console.aws.amazon.com/datazone 에 액세스하여 데이터 포털 URL을 확인할 수 있습니다.

2. 검색 옆의 상단 탐색 표시줄에서 카탈로그 메뉴로 이동합니다.
3. Amazon DataZone Data Portal에서 [메타데이터 양식] 을 선택한 다음 필드를 생성할 메타데이터 양식을 선택합니다.
4. 양식의 세부 정보 페이지에서 필드 생성을 선택합니다.
5. 필드 이름, 설명, 유형, 필수 필드인지 여부를 지정한 다음 필드 만들기를 선택합니다.

메타데이터 양식에서 필드를 편집하려면 다음 단계를 완료하세요.

1. 데이터 포털 URL을 사용하여 Amazon DataZone 데이터 포털로 이동하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생성된 AWS 계정의 Amazon DataZone 콘솔에서 https://console.aws.amazon.com/datazone 에 액세스하여 데이터 포털 URL을 확인할 수 있습니다.
2. 검색 옆의 상단 탐색 표시줄에서 카탈로그 메뉴로 이동합니다.
3. Amazon DataZone Data Portal에서 [메타데이터 양식] 을 선택한 다음 필드를 편집할 메타데이터 양식을 선택합니다.
4. 양식의 세부 정보 페이지에서 편집하려는 필드를 선택한 다음 작업을 확장하고 편집을 선택합니다.
5. 필드 이름, 설명, 유형 및 필수 필드인지 여부를 업데이트한 다음 필드 업데이트를 선택합니다.

메타데이터 양식에서 필드를 삭제하려면 다음 단계를 완료하세요.

1. 데이터 포털 URL을 사용하여 Amazon DataZone 데이터 포털로 이동하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생성된 AWS 계정의 Amazon DataZone 콘솔에서 https://console.aws.amazon.com/datazone 에 액세스하여 데이터 포털 URL을 확인할 수 있습니다.
2. 검색 옆의 상단 탐색 표시줄에서 카탈로그 메뉴로 이동합니다.
3. Amazon DataZone Data Portal에서 [메타데이터 양식] 을 선택한 다음 필드를 삭제하려는 메타데이터 양식을 선택합니다.
4. 양식의 세부 정보 페이지에서 삭제하려는 필드를 선택한 다음 작업을 확장하고 삭제를 선택합니다.
5. 삭제를 선택하여 삭제를 확인합니다.

Amazon의 프로젝트 및 환경 다루기 DataZone

Amazon에서는 프로젝트를 통해 사용자 그룹이 Amazon DataZone 카탈로그의 데이터 자산을 게시, 검색, 구독 및 사용하는 것과 관련된 다양한 비즈니스 사용 사례에 대해 협업할 수 있습니다. DataZone 각 Amazon DataZone 프로젝트에는 승인된 개인, 그룹 및 역할만 이 프로젝트가 구독하는 프로젝트 및 데이터 자산에 액세스하고 프로젝트 권한으로 정의된 도구만 사용할 수 있도록 일련의 액세스 제어가 적용됩니다. 프로젝트는 기본 리소스에 대한 액세스 권한을 받는 ID 주체 역할을 하므로 DataZone Amazon은 개별 사용자의 자격 증명에 의존하지 않고도 조직의 인프라 내에서 운영할 수 있습니다. 자세한 내용은 아마존 DataZone 용어 및 개념단원을 참조하세요.

주제

환경 프로필 생성

DataZoneAmazon에서 환경 프로파일은 환경을 생성하는 데 사용할 수 있는 템플릿입니다. 환경 프로필의 목적은 AWS 계정 및 지역과 같은 배치 정보를 프로필에 포함시켜 환경 생성을 단순화하는 것입니다. 자세한 정보는 아마존 DataZone 용어 및 개념을 참조하세요. Amazon DataZone 도메인에서 환경 프로필을 생성하려면 Amazon DataZone 프로젝트에 속해야 합니다. 모든 환경 프로필은 프로젝트가 소유하며, 모든 프로젝트의 승인된 모든 사용자가 새 환경을 만드는 데 사용할 수 있습니다.

환경 프로필을 만들려면

1. 데이터 포털 URL을 사용하여 Amazon DataZone 데이터 포털로 이동하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생성된 AWS 계정의 Amazon DataZone 콘솔에서 https://console.aws.amazon.com/datazone 에 액세스하여 데이터 포털 URL을 확인할 수 있습니다.
2. 데이터 포털 내에서 프로젝트 찾아보기를 선택하고 환경 프로파일을 생성할 프로젝트를 선택합니다.
3. 프로젝트 내의 환경 탭으로 이동한 다음 환경 프로필 생성을 선택합니다.
4. 다음 필드를 구성합니다.

   - 이름 - 환경 프로필의 이름입니다.
   - 설명 - (선택 사항) 환경 프로필에 대한 설명입니다.
   - 소유자 프로젝트 - 프로필이 생성되는 프로젝트가 이 필드에서 기본적으로 선택됩니다.
   - 블루프린트 — 이 프로필이 생성되는 블루프린트입니다. 기본 Amazon DataZone 블루프린트(데이터 레이크 또는 데이터 웨어하우스) 중 하나를 선택할 수 있습니다.

     데이터 웨어하우스 블루프린트를 지정한 경우 다음을 수행하십시오.

     - 파라미터 세트를 제공하십시오. 기존 파라미터 세트를 선택하려면 파라미터 세트 선택 옵션을 선택합니다. 직접 매개변수를 입력하려면 [직접 입력] 을 선택합니다.
     - 기존 매개변수를 선택하려는 경우 다음과 같이 하십시오.
       - 드롭다운에서 AWS 계정을 선택합니다.
       - 드롭다운에서 파라미터 세트를 선택합니다.
     - 매개변수를 직접 입력하기로 선택한 경우 다음과 같이 하십시오.
       - 드롭다운에서 AWS 계정 및 지역을 선택하여 AWS 매개변수를 입력합니다.
       - Redshift 데이터 웨어하우스 매개 변수를 제공하십시오.
         - Amazon Redshift 클러스터 또는 Amazon Redshift 서버리스를 선택합니다.
         - 선택한 Amazon Redshift 클러스터 또는 Amazon Redshift 서버리스 워크그룹에 대한 자격 증명이 들어 있는 AWS 보안 ARN을 입력합니다. AWS 암호에는 환경 프로필을 생성하는 도메인 ID 및 프로젝트 ID로 태그를 지정해야 합니다.
           - `AmazonDataZoneDomain: [Domain_ID]`
           - `AmazonDataZoneProject: [Project_ID]`
         - Amazon Redshift 클러스터 또는 Amazon Redshift 서버리스 워크그룹의 이름을 입력합니다.

- 선택한 Amazon Redshift 클러스터 또는 Amazon Redshift 서버리스 워크그룹 내의 데이터베이스 이름을 입력합니다.

- 승인된 프로젝트 섹션에서 환경 생성을 위해 환경 프로필을 사용할 수 있는 프로젝트를 지정합니다. 기본적으로 도메인 내의 모든 프로젝트는 계정의 환경 프로필을 사용하여 환경을 만들 수 있습니다. 이 기본 설정을 유지하려면 모든 프로젝트를 선택합니다. 하지만 승인된 프로젝트를 환경에 할당하여 이를 제한할 수 있습니다. 이렇게 하려면 승인된 프로젝트만을 선택한 다음 이 프로젝트 프로필을 사용하여 환경을 만들 수 있는 프로젝트를 지정하십시오.
- 게시 섹션에서 다음 옵션 중 하나를 선택합니다.
  - 모든 스키마에서 게시: 이 옵션을 선택하면 이 환경 프로필을 사용하여 만든 환경을 위에 제공된 Redshift 매개 변수에서 선택한 데이터베이스 내의 모든 스키마에서 게시하는 데 사용할 수 있습니다. 또한 이 환경 프로필을 사용하여 생성된 환경의 사용자는 자체 Amazon Redshift 파라미터를 제공하여 환경 프로필에서 선택한 AWS 계정 및 지역 내의 모든 스키마에서 게시할 수 있습니다.
  - 기본 환경 스키마에서만 게시: 이 옵션을 선택하면 이 옵션을 사용하여 만든 환경을 해당 환경에 DataZone 대해 Amazon에서 생성한 기본 스키마에서만 게시하는 데 사용할 수 있습니다. 이 환경 프로파일을 사용하여 생성된 환경의 사용자는 자신의 Amazon Redshift 파라미터를 제공할 수 없습니다.
  - 게시 허용 안 함: 이 옵션을 선택하면 이 환경 프로필을 사용하여 만든 환경을 구독 및 데이터 사용에만 사용할 수 있습니다. 환경을 사용하여 데이터를 전혀 게시할 수 없습니다.

Data Lake 블루프린트를 지정한 경우 다음을 수행하십시오.

- AWS 계정 매개 변수 섹션에서 잠재적 환경을 생성할 AWS AWS 계정 번호와 계정 지역을 지정합니다.
- 승인된 프로젝트 섹션에서 환경 생성을 위해 기본 제공되는 Data Lake 환경 프로필과 함께 환경 프로필을 사용할 수 있는 프로젝트를 지정합니다. 기본적으로 도메인 내의 모든 프로젝트는 계정의 데이터 레이크 블루프린트를 사용하여 환경 프로필을 만들 수 있습니다. 이 기본 설정을 유지하려면 모든 프로젝트를 선택합니다. 하지만 블루프린트에 프로젝트를 할당하여 이를 제한할 수 있습니다. 이렇게 하려면 승인된 프로젝트만을 선택한 다음 이 프로젝트 프로필을 사용하여 환경을 만들 수 있는 프로젝트를 지정하세요.
- 데이터베이스 섹션에서 모든 데이터베이스를 선택하여 환경이 생성된 AWS 계정 및 지역 내의 모든 데이터베이스에서 게시할 수 있도록 하거나 기본 데이터베이스만을 선택하여 해당 환경에서 만든 기본 게시 데이터베이스에서만 게시할 수 있도록 합니다.

5. 환경 프로필 만들기를 선택합니다.

환경 프로필 편집

DataZoneAmazon에서 환경 프로파일은 환경을 생성하는 데 사용할 수 있는 템플릿입니다. 자세한 정보는 아마존 DataZone 용어 및 개념을 참조하세요. Amazon DataZone 도메인의 기존 환경 프로필을 편집하려면 Amazon DataZone 프로젝트에 속해야 합니다.

환경 프로필을 편집하려면

1. Amazon DataZone 데이터 포털 URL로 이동하여 싱글 사인온 (SSO) 또는 자격 증명을 사용하여 로그인합니다. AWS Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 위치로 로그인한 다음 Open data portal을 선택할 수 있습니다.
2. 데이터 포털 내에서 프로젝트 찾아보기를 선택하고 환경 프로필을 편집하려는 프로젝트를 선택합니다.
3. 프로젝트 내의 환경 탭으로 이동한 다음 환경 프로필을 선택한 다음 편집하려는 환경 프로필을 선택합니다.

   Data Warehouse 환경 프로필을 편집하는 경우 기존 환경 프로필의 이름과 설명만 편집할 수 있습니다.

   Data Lake 환경 프로필을 편집하는 경우 프로필의 이름과 설명을 편집할 수 있으며 이 프로필을 사용하여 환경을 만들 권한이 있는 프로젝트를 편집하고 데이터베이스를 편집할 수도 있습니다. 이러한 설정을 편집하려면 다음과 같이 하십시오.

   - 승인된 프로젝트 섹션에서 환경 생성을 위해 기본 제공되는 Data Lake 환경 프로필과 함께 환경 프로필을 사용할 수 있는 프로젝트를 지정합니다. 기본적으로 도메인 내의 모든 프로젝트는 계정의 데이터 레이크 블루프린트를 사용하여 환경 프로필을 만들 수 있습니다. 이 기본 설정을 유지하려면 모든 프로젝트를 선택합니다. 하지만 블루프린트에 프로젝트를 할당하여 이를 제한할 수 있습니다. 이렇게 하려면 승인된 프로젝트만을 선택한 다음 이 프로젝트 프로필을 사용하여 환경을 만들 수 있는 프로젝트를 지정하세요.
   - 데이터베이스 섹션에서 모든 데이터베이스를 선택하여 환경이 생성된 AWS 계정 및 지역 내의 모든 데이터베이스에서 게시할 수 있도록 하거나 기본 데이터베이스만을 선택하여 해당 환경에서 만든 기본 게시 데이터베이스에서만 게시할 수 있도록 합니다.

   편집을 완료한 후 환경 프로필 편집을 선택합니다.

환경 프로필 삭제

DataZoneAmazon에서 환경 프로파일은 환경을 생성하는 데 사용할 수 있는 템플릿입니다. 환경 프로필의 목적은 AWS 계정 및 지역과 같은 배치 정보를 프로필에 포함시켜 환경 생성을 단순화하는 것입니다. 자세한 정보는 아마존 DataZone 용어 및 개념을 참조하세요. Amazon DataZone 도메인에서 환경 프로필을 삭제하려면 Amazon DataZone 프로젝트에 속해야 합니다.

> **Note**
>
> 환경 프로필을 삭제하면 이 프로필을 사용하여 더 이상 환경을 만들 수 없습니다.

환경 프로필을 삭제하려면

1. Amazon DataZone 데이터 포털 URL로 이동하여 싱글 사인온 (SSO) 또는 자격 증명을 사용하여 로그인합니다. AWS Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 위치로 로그인한 다음 Open data portal을 선택할 수 있습니다.
2. 데이터 포털 내에서 프로젝트 찾아보기를 선택하고 환경 프로필을 삭제하려는 프로젝트를 선택합니다.
3. 프로젝트 내의 환경 탭으로 이동한 다음 환경 프로필을 선택한 다음 삭제하려는 환경 프로필을 선택합니다.
4. 삭제하려는 환경 프로필을 선택한 다음 작업, 삭제를 선택하고 삭제를 확인합니다.

새 환경 만들기

Amazon DataZone 프로젝트에서 환경은 구성된 리소스 모음 (예: Amazon S3 버킷, AWS Glue 데이터베이스 또는 Amazon Athena 작업 그룹) 이며, 해당 리소스를 운영할 수 있는 소유자 또는 기여자 권한이 지정된 IAM 보안 주체 세트 (환경 사용자 역할) 가 있습니다. 자세한 정보는 아마존 DataZone 용어 및 개념을 참조하세요.

데이터 포털에 액세스하는 데 필요한 권한을 가진 모든 Amazon DataZone 사용자는 프로젝트 내에 Amazon DataZone 환경을 만들 수 있습니다.

새 환경을 만들려면 다음 단계를 완료하십시오.

1. Amazon DataZone 데이터 포털 URL로 이동하여 싱글 사인온 (SSO) 또는 자격 증명을 사용하여 로그인합니다. AWS Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/

datazone 에서 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 위치로 로그인한 다음 Open data portal을 선택할 수 있습니다.

2. [모든 프로젝트 찾아보기] 를 선택하고 새 환경을 만들려는 프로젝트를 선택합니다.
3. 환경 만들기를 선택하고 다음 필드에 값을 지정한 다음 환경 만들기를 선택합니다.

   - 이름 - 환경 이름
   - 설명 — 환경에 대한 설명
   - 환경 프로필 — 기존 환경 프로필을 선택하거나 새 환경 프로필을 생성합니다. 환경 프로필은 환경을 만드는 데 사용할 수 있는 템플릿입니다. 자세한 정보는 아마존 DataZone 용어 및 개념을 참조하세요.

     환경 프로필을 선택한 후에는 매개 변수 섹션에서 이 환경 프로필에 속하는 필드의 값을 지정합니다.

환경 편집

Amazon DataZone 프로젝트에서 환경은 구성된 리소스 모음 (예: Amazon S3 버킷, AWS Glue 데이터베이스 또는 Amazon Athena 작업 그룹) 이며, 해당 리소스를 운영할 수 있는 지정된 IAM 보안 주체 세트 (기여자 권한이 할당됨) 가 있습니다. 자세한 정보는 아마존 DataZone 용어 및 개념을 참조하세요.

데이터 포털에 액세스하는 데 필요한 권한을 가진 모든 Amazon DataZone 사용자는 프로젝트 내에서 Amazon DataZone 환경을 편집할 수 있습니다.

기존 환경을 편집하려면 다음 단계를 완료하십시오.

1. Amazon DataZone 데이터 포털 URL로 이동하여 싱글 사인온 (SSO) 또는 자격 증명을 사용하여 로그인합니다. AWS Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 위치로 로그인한 다음 Open data portal을 선택할 수 있습니다.
2. 상단 탐색 창에서 프로젝트 찾아보기를 선택하고 편집하려는 환경이 포함된 프로젝트를 선택합니다.
3. 환경을 찾아 선택하여 해당 세부 정보 페이지를 엽니다. 그런 다음 작업을 확장하고 환경 편집을 선택합니다.
4. 환경 이름 및 설명을 편집한 다음 변경 내용 저장을 선택합니다.

환경을 삭제합니다.

Amazon DataZone 프로젝트에서 환경은 구성된 리소스 모음 (예: Amazon S3 버킷, AWS Glue 데이터베이스 또는 Amazon Athena 작업 그룹) 이며, 해당 리소스를 운영할 수 있는 지정된 IAM 보안 주체 세트 (기여자 권한이 할당됨) 가 있습니다. 자세한 정보는 아마존 DataZone 용어 및 개념을 참조하세요.

데이터 포털에 액세스하는 데 필요한 권한을 가진 모든 Amazon DataZone 사용자는 프로젝트 내에서 Amazon DataZone 환경을 삭제할 수 있습니다.

기존 환경을 삭제하려면 다음 단계를 완료하십시오.

1. Amazon DataZone 데이터 포털 URL로 이동하여 싱글 사인온 (SSO) 또는 자격 증명을 사용하여 로그인합니다. AWS Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 위치로 로그인한 다음 Open data portal을 선택할 수 있습니다.
2. 상단 탐색 창에서 프로젝트 찾아보기를 선택하고 삭제하려는 환경이 포함된 프로젝트를 선택합니다.
3. 환경을 찾아 선택하여 세부 정보 페이지를 연 다음 작업을 확장하고 환경 삭제를 선택합니다.
4. 환경 삭제 팝업 창에서 필드에 입력하여 `Delete` 삭제를 확인한 다음 환경 삭제를 선택합니다.

   해당 환경에 종속된 모든 개체가 삭제된 후에만 환경을 성공적으로 삭제할 수 있습니다. 환경을 삭제하려면 먼저 관련 데이터 소스 및 구독 대상을 모두 삭제해야 합니다.

새 프로젝트 만들기

Amazon에서는 프로젝트를 통해 사용자 그룹이 Amazon DataZone 카탈로그의 데이터 자산을 게시, 검색, 구독 및 사용하는 것과 관련된 다양한 비즈니스 사용 사례에 대해 협업할 수 있습니다. DataZone 자세한 정보는 아마존 DataZone 용어 및 개념을 참조하세요.

데이터 포털에 액세스하는 데 필요한 권한을 가진 모든 Amazon DataZone 사용자는 Amazon DataZone 프로젝트를 생성할 수 있습니다.

새 프로젝트를 생성하려면 다음 단계를 완료하십시오.

1. Amazon DataZone 데이터 포털 URL로 이동하여 싱글 사인온 (SSO) 또는 자격 증명을 사용하여 로그인합니다. AWS Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 위치로 로그인한 다음 Open data portal을 선택할 수 있습니다.

2. Amazon DataZone 데이터 포털에서 [프로젝트 생성] 을 선택합니다.
3. 다음 필드의 값을 지정한 다음 [Create project] 를 선택합니다.

   - 이름 - 프로젝트 이름.
   - 설명 — 프로젝트에 대한 설명.

프로젝트 편집

Amazon에서는 프로젝트를 통해 사용자 그룹이 Amazon DataZone 카탈로그의 데이터 자산을 게시, 검색, 구독 및 사용하는 것과 관련된 다양한 비즈니스 사용 사례에 대해 협업할 수 있습니다. DataZone 자세한 정보는 아마존 DataZone 용어 및 개념을 참조하세요. Amazon DataZone 프로젝트를 편집하려면 해당 프로젝트의 소유자 또는 이 프로젝트가 포함된 도메인의 도메인 관리자여야 합니다.

기존 프로젝트를 편집하려면 다음 단계를 완료하십시오.

1. Amazon DataZone 데이터 포털 URL로 이동하여 싱글 사인온 (SSO) 또는 자격 증명을 사용하여 로그인합니다. AWS Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 위치로 로그인한 다음 Open data portal을 선택할 수 있습니다.
2. 프로젝트 찾아보기를 선택합니다.
3. 편집하려는 프로젝트를 선택합니다. 프로젝트 목록에서 해당 프로젝트가 쉽게 보이지 않는 경우, 프로젝트 찾기 필드에 프로젝트 이름을 지정하여 검색할 수 있습니다.
4. 작업을 펼치고 프로젝트 편집을 선택합니다.
5. 프로젝트 이름과 설명을 업데이트한 다음 저장을 선택합니다.

프로젝트 삭제

Amazon에서는 프로젝트를 통해 사용자 그룹이 Amazon DataZone 카탈로그의 데이터 자산을 게시, 검색, 구독 및/또는 사용하는 것과 관련된 다양한 비즈니스 사용 사례에 대해 협업할 수 있습니다. DataZone 자세한 정보는 아마존 DataZone 용어 및 개념을 참조하세요.

프로젝트 삭제는 최종적입니다. 삭제하면 데이터 소스, 환경, 자산, 용어집, 메타데이터 양식을 비롯한 프로젝트 콘텐츠가 영구적으로 삭제됩니다. DataZone 아마존은 아마존이 Lake Formation과 Amazon DataZone Redshift를 통해 관리 자산에 지급한 보조금을 취소합니다. 프로젝트를 삭제해도 Amazon에서 생성하는 데 도움을 준 Amazon DataZone 외 DataZone AWS 리소스는 삭제되지 않습니다. 이러한 AWS 리소스가 더 이상 필요하지 않은 경우 해당 AWS 서비스 및 계정에서 삭제하십시오.

Amazon DataZone 프로젝트를 삭제하려면 프로젝트 소유자여야 합니다.

기존 프로젝트를 삭제하려면 다음 단계를 완료하십시오.

1. Amazon DataZone 데이터 포털 URL로 이동하여 싱글 사인온 (SSO) 또는 자격 증명을 사용하여 로그인합니다. AWS IAM 주체는 https://console.aws.amazon.com/datazone Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 위치로 로그인한 다음 Open data portal을 선택하면 됩니다.
2. 상단 탐색 창에서 프로젝트 찾아보기를 선택합니다.
3. 삭제하려는 프로젝트를 선택합니다. 프로젝트 목록에 표시되지 않는 경우 프로젝트 찾기 필드에 프로젝트 이름을 지정하여 검색할 수 있습니다.
4. 작업을 펼치고 프로젝트 삭제를 선택합니다.

   프로젝트 삭제의 잠재적 영향에 대한 정보 제공 경고를 검토하세요.
5. 경고를 수락하면 확인 텍스트를 입력하고 삭제를 선택합니다.

> **Important**
>
> 프로젝트 삭제는 취소할 수 없는 작업이며 직접 또는 직접 취소할 수 없습니다. AWS

> **Note**
>
> 귀하 또는 도메인 사용자가 프로젝트에 환경을 만들면 Amazon은 도메인 또는 관련 계정에 AWS 리소스를 DataZone 생성하여 귀하와 도메인 사용자에게 기능을 제공합니다. 다음은 Amazon이 프로젝트용으로 생성할 DataZone 수 있는 AWS 리소스 목록과 기본 이름입니다. 프로젝트를 삭제해도 AWS 계정에서 이러한 AWS 리소스는 삭제되지 않습니다.
>
> - <environmentId>IAM 역할: datazone_usr_.
> - <environmentName>글루 데이터베이스: (1) <environmentName>_pub_db-*, (2) _sub_db-*. 이 이름의 기존 데이터베이스가 이미 있는 경우 DataZone Amazon은 환경 ID를 추가합니다.
> - <environmentName>Athena 워크그룹: -*. 이 이름의 기존 워크그룹이 이미 있는 경우 DataZone Amazon은 환경 ID를 추가합니다.
> - CloudWatch 로그 그룹: 데이터존_ <environmentId>

프로젝트 탈퇴

Amazon에서는 프로젝트를 통해 사용자 그룹이 Amazon DataZone 카탈로그의 데이터 자산을 게시, 검색, 구독 및 사용하는 것과 관련된 다양한 비즈니스 사용 사례에 대해 협업할 수 있습니다. DataZone 자세한 정보는 아마존 DataZone 용어 및 개념을 참조하세요.

기존 프로젝트에서 탈퇴하려면 다음 단계를 완료하십시오.

1. Amazon DataZone 데이터 포털 URL로 이동하여 싱글 사인온 (SSO) 또는 자격 증명을 사용하여 로그인합니다. AWS Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 위치로 로그인한 다음 Open data portal을 선택할 수 있습니다.
2. 상단 탐색 창에서 프로젝트 선택을 선택하고 프로젝트를 선택합니다.
3. 탈퇴하려는 프로젝트를 선택합니다. 프로젝트 목록에서 해당 프로젝트가 쉽게 보이지 않는 경우, 프로젝트 찾기 필드에 프로젝트 이름을 지정하여 검색할 수 있습니다.
4. 작업을 펼치고 프로젝트 탈퇴를 선택합니다.

프로젝트에 구성원 추가

Amazon에서는 프로젝트를 통해 사용자 그룹이 Amazon DataZone 카탈로그의 데이터 자산을 게시, 검색, 구독 및 사용하는 것과 관련된 다양한 비즈니스 사용 사례에 대해 협업할 수 있습니다. DataZone 자세한 정보는 아마존 DataZone 용어 및 개념을 참조하세요.

프로젝트에 멤버를 추가하려면 프로젝트 소유자 또는 기여자여야 합니다. SSO 그룹, SSO 사용자 또는 IAM 주도자 (역할 또는 사용자) 를 프로젝트 구성원으로 추가할 수 있습니다.

기존 프로젝트에 구성원을 추가하려면 다음 단계를 완료하세요.

1. Amazon DataZone 데이터 포털 URL로 이동하여 싱글 사인온 (SSO) 또는 자격 증명을 사용하여 로그인합니다. AWS Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 위치로 로그인한 다음 Open data portal을 선택할 수 있습니다.
2. 상단 탐색 창에서 프로젝트 선택을 선택하고 프로젝트를 선택합니다.
3. 멤버를 추가하려는 프로젝트를 선택합니다. 프로젝트 목록에서 쉽게 찾을 수 없는 경우 프로젝트 찾기 필드에 프로젝트 이름을 지정하여 검색할 수 있습니다.
4. 프로젝트의 세부정보 페이지에서 멤버 탭을 선택하고 모든 멤버 선택 노드를 선택합니다.

5. 프로젝트 멤버 탭에서 멤버 추가를 선택합니다.
6. 프로젝트에 구성원 추가 팝업 창에서 추가하려는 사용자를 지정하고 프로젝트 내에서의 역할 (소유자 또는 기여자) 을 지정한 다음 구성원 추가를 선택합니다.

> **Note**
>
> IAM 보안 주체 도메인에 이미 Amazon DataZone 사용자 프로필이 있는 경우 IAM 보안 주체를 프로젝트 구성원으로 추가할 수 있습니다. Amazon은 IAM 보안 주체가 포털, API 또는 CLI를 통해 도메인과 성공적으로 상호 작용하면 IAM 보안 주체에 대한 사용자 프로필을 DataZone 자동으로 생성합니다. IAM 보안 주체에 대한 사용자 프로필은 생성할 수 없습니다. IAM 보안 주체에 도메인에 기존 Amazon DataZone 사용자 프로필이 없는 경우 IAM 보안 주체를 프로젝트 구성원으로 추가하려면 관리자에게 IAM 콘솔에서 다음 두 개의 IAM 권한을 도메인에 추가하도록 요청하세요. AmazonDataZoneDomainExecutionRole`iam:GetUser`iam:GetRole 이와 별도로, 도메인에서 작업을 수행하려면 IAM 주체는 해당 작업에 해당하는 IAM 권한을 가지고 있어야 합니다.

프로젝트에서 구성원 제거

Amazon에서는 프로젝트를 통해 사용자 그룹이 Amazon DataZone 카탈로그의 데이터 자산을 게시, 검색, 구독 및 사용하는 것과 관련된 다양한 비즈니스 사용 사례에 대해 협업할 수 있습니다. DataZone 자세한 정보는 아마존 DataZone 용어 및 개념을 참조하세요. 프로젝트에서 멤버를 제거하려면 프로젝트 소유자여야 합니다.

기존 프로젝트에서 멤버를 제거하려면 다음 단계를 완료하세요.

1. 데이터 포털 URL을 사용하여 Amazon DataZone 데이터 포털로 이동하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생성된 AWS 계정의 Amazon DataZone 콘솔에서 https://console.aws.amazon.com/datazone 에 액세스하여 데이터 포털 URL을 확인할 수 있습니다.
2. 상단 탐색 창에서 프로젝트 선택을 선택하고 프로젝트를 선택합니다.
3. 구성원을 제거하려는 프로젝트를 선택합니다. 프로젝트 목록에서 쉽게 찾을 수 없는 경우 프로젝트 찾기 필드에 프로젝트 이름을 지정하여 검색할 수 있습니다.
4. 프로젝트의 세부정보 페이지에서 멤버 탭을 선택하고 모든 멤버 선택 노드를 선택합니다.
5. 프로젝트 멤버 탭에서 프로젝트에서 제거하려는 멤버를 선택한 다음 제거를 선택합니다.
6. 구성원 제거 팝업 창에서 구성원 제거를 선택하여 제거를 확인합니다.

Amazon에서 인벤토리 생성 및 데이터 게시 DataZone

이 섹션에서는 Amazon에서 데이터 인벤토리를 생성하고 Amazon에 데이터를 게시하기 위해 수행하려는 DataZone 작업과 절차를 설명합니다 DataZone.

DataZone Amazon을 사용하여 데이터를 카탈로그화하려면 먼저 데이터 (자산) 를 프로젝트 인벤토리로 Amazon에 가져와야 DataZone 합니다. 특정 프로젝트에 대한 인벤토리를 생성하면 해당 프로젝트 구성원만 자산을 검색할 수 있습니다. 명시적으로 게시되지 않는 한 모든 도메인 사용자가 검색/찾아보기에서 프로젝트 인벤토리 자산을 사용할 수 있는 것은 아닙니다. 프로젝트 인벤토리를 생성한 후 데이터 소유자는 비즈니스 이름 (자산 및 스키마), 설명 (자산 및 스키마), Read Me, 용어집 용어 (자산 및 스키마), 메타데이터 양식을 추가하거나 업데이트하여 필요한 비즈니스 메타데이터를 사용하여 인벤토리 자산을 관리할 수 있습니다.

Amazon을 사용하여 데이터를 DataZone 카탈로그화하는 다음 단계는 프로젝트의 인벤토리 자산을 도메인 사용자가 검색할 수 있도록 하는 것입니다. 아마존 DataZone 카탈로그에 인벤토리 자산을 게시하여 이 작업을 수행할 수 있습니다. 인벤토리 자산의 최신 버전만 카탈로그에 게시할 수 있으며 가장 최근에 게시된 버전만 검색 카탈로그에서 활성화됩니다. 재고 자산이 아마존 DataZone 카탈로그에 게시된 후 업데이트되는 경우, 검색 카탈로그에 최신 버전이 포함되도록 하려면 이를 다시 명시적으로 게시해야 합니다.

주제

- 아마존의 데이터 품질 DataZone
- 머신 러닝 및 제너레이티브 AI 사용

Amazon에 대한 Lake Formation 권한 구성 DataZone

내장된 데이터 레이크 blueprint (DefaultDataLake) 를 사용하여 환경을 생성하면 이 환경 생성 프로세스의 DataZone 일부로 Amazon에 AWS Glue 데이터베이스가 추가됩니다. 이 AWS Glue 데이터베이스의 자산을 게시하려는 경우 추가 권한이 필요하지 않습니다.

하지만 Amazon DataZone 환경 외부에 있는 AWS Glue 데이터베이스의 자산을 게시하고 자산을 구독하려면 Amazon에 이 외부 AWS Glue 데이터베이스의 테이블에 액세스할 수 DataZone 있는 권한을 명시적으로 제공해야 합니다. 이렇게 하려면 Lake Formation에서 다음 설정을 완료하고 필요한 AWS Lake Formation 권한을 에 첨부해야 AmazonDataZoneGlueAccess- <region>- <domainId> 합니다.

- Lake Formation 권한 모드 또는 하이브리드 액세스 모드를 사용하여 AWS Lake Formation의 데이터 레이크에 대한 Amazon S3 위치를 구성합니다. 자세한 내용은 https://docs.aws.amazon.com/lake-formation/latest/dg/ register-data-lake .html을 참조하십시오.
- 아마존이 `IAMAllowedPrincipals` 권한을 DataZone 처리하는 Amazon Lake Formation 테이블에서 권한을 제거합니다. 자세한 내용은 https://docs.aws.amazon.com/lake-formation/latest/dg/upgrade-glue-lake-formation -background.html 를 참조하십시오.
- 다음 AWS Lake Formation 권한을 AmazonDataZoneGlueAccess- <region>- <domainId> 다음 사이트에 첨부하십시오.
  - `Describe`및 테이블이 있는 데이터베이스에 대한 `Describe grantable` 권한
  - `DescribeSelect`,`Describe Grantable`,, `Select Grantable` 사용자를 대신하여 액세스를 DataZone 관리하려는 위 데이터베이스의 모든 테이블에 대한 권한.

> **Note**
>
> DataZone Amazon은 AWS Lake Formation 하이브리드 모드를 지원합니다. Lake Formation 하이브리드 모드를 사용하면 Lake Formation을 통해 AWS Glue 데이터베이스 및 테이블에 대한 권한 관리를 시작하는 동시에 이러한 테이블과 데이터베이스에 대한 기존 IAM 권한을 계속 유지할 수 있습니다. 자세한 내용은 아마존과 AWS 레이크 포메이션 하이브리드 모드 DataZone 통합 단원을 참조하세요.

자세한 정보는 Amazon의 AWS Lake Formation 권한 문제 해결 DataZone을 참조하세요.

아마존과 AWS 레이크 포메이션 하이브리드 모드 DataZone 통합

DataZone Amazon은 AWS Lake Formation 하이브리드 모드와 통합되어 있습니다. 이 통합을 통해 AWS Lake Formation에 먼저 등록할 필요 DataZone 없이 Amazon을 통해 AWS Glue 테이블을 쉽게 게시하고 공유할 수 있습니다. 하이브리드 모드를 사용하면 AWS Lake Formation을 통해 AWS Glue 테이블에 대한 권한 관리를 시작하면서 해당 테이블에 대한 기존 IAM 권한을 계속 유지할 수 있습니다.

시작하려면 Amazon DataZone 관리 콘솔의 DefaultDataLake블루프린트에서 데이터 위치 등록 설정을 활성화하면 됩니다.

AWS Lake Formation 하이브리드 모드와의 통합 지원

1. https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 계정 자격 증명으로 로그인합니다.
2. 도메인 보기를 선택하고 AWS Lake Formation 하이브리드 모드와의 통합을 활성화하려는 도메인을 선택합니다.
3. 도메인 세부정보 페이지에서 블루프린트 탭으로 이동합니다.
4. 블루프린트 목록에서 블루프린트를 선택합니다. DefaultDataLake
5. DefaultDataLake 블루프린트가 활성화되어 있는지 확인하세요. 활성화되지 않은 경우, 단계에 따라 AWS 계정에서 Amazon 도메인을 소유한 AWS 계정에서 빌트인 블루프린트를 활성화합니다. DataZone 활성화하세요.
6. DefaultDataLake 세부 정보 페이지에서 프로비저닝 탭을 열고 페이지 오른쪽 상단의 편집 버튼을 선택합니다.
7. 데이터 위치 등록에서 확인란을 선택하여 데이터 위치 등록을 활성화합니다.
8. 데이터 위치 관리 역할의 경우 새 IAM 역할을 만들거나 기존 IAM 역할을 선택할 수 있습니다. DataZone Amazon은 이 역할을 사용하여 AWS Lake Formation 하이브리드 액세스 모드를 사용하는 Data Lake용으로 선택한 Amazon S3 버킷에 대한 읽기/쓰기 액세스를 관리합니다. 자세한 정보는 AmazonDataZone<region>S3Manage- - <domainId>을 참조하세요.
9. Amazon이 하이브리드 모드에서 특정 Amazon S3 위치를 자동으로 등록하지 않도록 하려면 선택적으로 특정 Amazon DataZone S3 위치를 제외하도록 선택할 수 있습니다. 이를 위해 다음 단계를 완료하십시오.
   - 토글 버튼을 선택하여 지정된 Amazon S3 위치를 제외합니다.
   - 제외하려는 Amazon S3 버킷의 URI를 입력합니다.
   - 버킷을 더 추가하려면 [S3 위치 추가] 를 선택합니다.

> **Note**
>
> Amazon은 루트 S3 DataZone 위치만 제외할 수 있습니다. 루트 S3 위치 경로에 있는 모든 S3 위치는 등록에서 자동으로 제외됩니다.

- 변경 사항 저장를 선택합니다.

AWS 계정에서 데이터 위치 등록 설정을 활성화한 후 데이터 소비자가 IAM 권한을 통해 관리되는 AWS Glue 테이블을 DataZone 구독하면 Amazon은 먼저 하이브리드 모드에서 이 테이블의 Amazon S3 위치를 등록한 다음 AWS Lake Formation을 통해 테이블에 대한 권한을 관리하여 데이터 소비자에게 액세스 권한을 부여합니다. 이렇게 하면 기존 워크플로에 영향을 주지 않으면서 테이블에 대한 IAM 권한이 새로 부여된 AWS Lake Formation 권한을 사용해도 계속 유지됩니다.

Amazon에서 AWS Lake Formation 하이브리드 모드 통합을 활성화할 때 암호화된 Amazon S3 위치를 처리하는 방법 DataZone

고객 관리형 또는 AWS 관리형 KMS 키로 암호화된 Amazon S3 위치를 사용하는 경우, AmazonDataZoneS3Manage 역할에 KMS 키로 데이터를 암호화하고 해독할 권한이 있거나, KMS 키 정책에서 키에 대한 권한을 역할에 부여해야 합니다.

Amazon S3 위치가 AWS 관리 키로 암호화된 경우 다음 인라인 정책을 AmazonDataZoneDataLocationManagement역할에 추가하십시오.

```
 {
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "kms:Encrypt",
      "kms:Decrypt",
      "kms:ReEncrypt*",
      "kms:GenerateDataKey*",
      "kms:DescribeKey"
    ],
    "Resource": "<AWS managed key ARN>"
  }
]
```

Amazon S3 위치가 고객 관리 키로 암호화된 경우, 다음을 수행하십시오.

1. https://console.aws.amazon.com/kms 에서 AWS KMS 콘솔을 열고 AWS Identity 및 Access Management (IAM) 관리 사용자 또는 위치를 암호화하는 데 사용되는 KMS 키의 키 정책을 수정할 수 있는 사용자로 로그인합니다.
2. 탐색 창에서 고객 관리형 키를 선택한 다음 원하는 KMS 키의 이름을 선택합니다.
3. KMS 키 세부 정보 페이지에서 키 정책 탭을 선택한 다음 다음 중 하나를 수행하여 사용자 지정 역할 또는 Lake Formation 서비스 연결 역할을 KMS 키 사용자로 추가합니다.

   - 기본 보기 (키 관리자, 키 삭제, 키 사용자, 기타 AWS 계정 섹션 포함) 가 표시되면 키 사용자 섹션 아래에 역할을 추가합니다. AmazonDataZoneDataLocationManagement
   - 키 정책 (JSON) 이 표시되는 경우 다음 예와 같이 정책을 편집하여 '키 사용 허용' 객체에 AmazonDataZoneDataLocationManagement역할을 추가합니다.

```
...
        {
            "Sid": "Allow use of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:role/service-role/
AmazonDataZoneDataLocationManage-<region>-<domain-id>",
                    "arn:aws:iam::111122223333:user/keyuser"
                ]
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        },
        ...
```

> **Note**
>
> KMS 키 또는 Amazon S3 위치가 데이터 카탈로그와 동일한 AWS 계정에 있지 않은 경우 AWS 계정 전체에 암호화된 Amazon S3 위치 등록의 지침을 따르십시오.

사용자 지정 자산 유형 생성

Amazon에서 자산은 데이터베이스 테이블 DataZone, 대시보드 또는 기계 학습 모델과 같은 특정 유형의 데이터 리소스를 나타냅니다. 카탈로그 자산을 설명할 때 일관성과 표준화를 제공하려면 Amazon DataZone 도메인에는 자산이 카탈로그에 표시되는 방식을 정의하는 자산 유형 세트가 있어야 합니다. 자산 유형은 특정 유형의 자산에 대한 스키마를 정의합니다. 자산 유형에는 이름을 지정할 수 있는 필수 및 선택적 메타데이터 양식 유형 세트 (예: GovForm 또는 GovernanceFormType) 가 있습니다. Amazon의 자산 유형에는 버전이 DataZone 지정되어 있습니다. 자산이 생성되면 자산 유형 (일반적으로 최신 버전) 으로 정의된 스키마를 기준으로 검증되며, 잘못된 구조가 지정되면 자산 생성이 실패합니다.

시스템 자산 유형 - Amazon은 서비스 소유 시스템 자산 유형 (GlueTableAssetType,,, GlueViewAssetType RedshiftTableAssetType RedshiftViewAssetType, S3 포함 ObjectCollectionAssetType) 과 시스템 양식 유형 (DataSourceReferenceFormType AssetCommonDetailsFormType, 및 SubscriptionTermsFormType 포함) 을 DataZone 프로비저닝합니다. 시스템 자산 유형은 편집할 수 없습니다.

사용자 지정 자산 유형 - 사용자 지정 자산 유형을 만들려면 먼저 양식 유형에 사용할 필수 메타데이터 양식 유형과 용어집을 만들어야 합니다. 그런 다음 이름, 설명 및 관련 메타데이터 양식 (필수 또는 선택 사항) 을 지정하여 사용자 지정 자산 유형을 만들 수 있습니다.

구조화된 데이터가 포함된 자산 유형의 경우 데이터 포털의 열 스키마를 나타내기 `RelationalTableFormType` 위해 를 사용하여 열에 기술 메타데이터 (열 이름, 설명, 데이터 유형 등) 를 추가하고 비즈니스 이름, 용어집 용어, 사용자 지정 키 값 쌍을 비롯한 열의 비즈니스 설명을 추가할 수 있습니다. `ColumnBusinessMetadataForm`

데이터 포털을 통해 사용자 지정 자산 유형을 생성하려면 다음 단계를 완료하세요.

1. Amazon DataZone 데이터 포털 URL로 이동하여 싱글 사인온 (SSO) 또는 자격 증명을 사용하여 로그인합니다. AWS Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 위치로 로그인한 다음 Open data portal을 선택할 수 있습니다.

2. 상단 탐색 창에서 프로젝트 선택을 선택하고 사용자 지정 자산 유형을 생성하려는 프로젝트를 선택합니다.
3. 프로젝트의 데이터 탭으로 이동합니다.
4. 왼쪽 탐색 창에서 자산 유형을 선택한 다음 자산 유형 만들기를 선택합니다.
5. 다음을 지정한 다음 [Create] 를 선택합니다.
   - 이름 - 사용자 지정 에셋 유형의 이름
   - 설명 - 사용자 지정 자산 유형에 대한 설명.
   - 메타데이터 양식 추가를 선택하여 이 사용자 지정 자산 유형에 메타데이터 양식을 추가합니다.
6. 사용자 지정 자산 유형을 만든 후에는 이를 사용하여 자산을 만들 수 있습니다.

API를 통해 사용자 지정 자산 유형을 만들려면 다음 단계를 완료하세요.

1. `CreateFormType`API 작업을 호출하여 메타데이터 양식 유형을 생성합니다.

   다음은 Amazon의 SageMaker 예시입니다.

```
m_model = "

structure SageMakerModelFormType {
   @required
   @amazon.datazone#searchable
   modelName: String

   @required
   modelArn: String

   @required
   creationTime: String
}
"

CreateFormType(
    domainIdentifier="my-dz-domain",
    owningProjectIdentifier="d4bywm0cja1dbb",
    name="SageMakerModelFormType",
    model=m_model
    status="ENABLED"
    )
```

2. 다음으로 CreateAssetType API 작업을 호출하여 자산 유형을 생성할 수 있습니다. 사용 가능한 시스템 양식 유형 (SubscriptionTermsFormType아래 예) 또는 사용자 지정 양식 유형을 사용하여 Amazon DataZone API를 통해서만 자산 유형을 생성할 수 있습니다. 시스템 양식 유형의 경우 유형 이름은 로 amazon.datazone 시작해야 합니다.

```
CreateAssetType(
    domainIdentifier="my-dz-domain",
    owningProjectIdentifier="d4bywm0cja1dbb",
    name="SageMakerModelAssetType",
    formsInput={
        "ModelMetadata": {
            "typeIdentifier": "SageMakerModelMetadataFormType",
            "typeRevision": 7,
            "required": True,
        },
        "SubscriptionTerms": {
            "typeIdentifier": "amazon.datazone.SubscriptionTermsFormType",
            "typeRevision": 1,
            "required": False,
        },
    },
)
```

다음은 구조화된 데이터용 자산 유형을 만드는 예시입니다.

```
CreateAssetType(
    domainIdentifier="my-dz-domain",
    owningProjectIdentifier="d4bywm0cja1dbb",
    name="OnPremMySQLAssetType",
    formsInput={
        "OnpremMySQLForm": {
            "typeIdentifier": "OnpremMySQLFormType",
            "typeRevision": 5,
            "required": True,
        },
        "RelationalTableForm": {
```

```
            "typeIdentifier": "RelationalTableFormType",
            "typeRevision": 1,
            "required": True,
        },
        "ColumnBusinessMetadataForm": {
            "typeIdentifier": "ColumnBusinessMetadataForm",
            "typeRevision": 1,
            "required": False,
        },
        "SubscriptionTerms": {
            "typeIdentifier": "SubscriptionTermsFormType",
            "typeRevision": 1,
            "required": False,
        },
    },
)
```

3. 이제 위 단계에서 만든 사용자 지정 자산 유형을 사용하여 자산을 만들 수 있습니다.

```
CreateAsset(
   domainIdentifier="my-dz-domain",
   owningProjectIdentifier="d4bywm0cja1dbb",
   owningProjectIdentifier="my-project",
   name="MyModelAsset",
   glossaryTerms="xxx",
   formsInput=[{
        "formName": "SageMakerModelForm",
        "typeIdentifier": "SageMakerModelForm",
        "typeRevision": "5",
        "content": "{\n \"ModelName\" : \"sample-ModelName\",\n \"ModelArn\" :
 \"999999911111\"\n}"
        }
        ]
)
```

이 예시에서는 구조화된 데이터 자산을 만들고 있습니다.

```
CreateAsset(
```

```
    domainIdentifier="my-dz-domain",
    owningProjectIdentifier="d4bywm0cja1dbb",
    name="MyModelAsset",
    glossaryTerms="xxx",
    formsInput=[{
         "formName": "RelationalTableForm",
         "typeIdentifier": "amazon.datazone.RelationalTableForm",
         "typeRevision": "1",
         "content": ".."
         },
         {
         "formName": "mySQLTableForm",
         "typeIdentifier": "mySQLTableForm",
         "typeRevision": "6",
         "content": ".."
         },
         {
         "formName": "mySQLTableForm",
         "typeIdentifier": "mySQLTableForm",
         "typeRevision": "1",
         "content": ".."
         },
         .....
         ]
)
```

다음을 위한 Amazon DataZone 데이터 소스 생성 및 실행 AWS Glue Data Catalog

DataZoneAmazon에서는 데이터베이스 테이블의 기술 AWS Glue Data Catalog 메타데이터를 가져오기 위해 데이터 소스를 생성할 수 AWS Glue있습니다. 에 대한 데이터 소스를 추가하려면 원본 데이터베이스가 이미 있어야 합니다 AWS Glue. AWS Glue Data Catalog

AWS Glue 데이터 소스를 생성하고 실행할 때 원본 AWS Glue 데이터베이스의 자산을 Amazon DataZone 프로젝트 인벤토리에 추가합니다. 정해진 일정에 따라 또는 필요에 따라 AWS Glue 데이터 소스를 실행하여 자산의 기술 메타데이터를 생성하거나 업데이트할 수 있습니다. 데이터 소스를 실행하는 동안 선택적으로 자산을 Amazon DataZone 카탈로그에 게시하여 모든 도메인 사용자가 검색할 수 있도록 할 수 있습니다. 비즈니스 메타데이터를 편집한 후 프로젝트 인벤토리 자산을 게시할 수도

있습니다. 도메인 사용자는 게시된 자산을 검색 및 검색하고 해당 자산에 대한 구독을 요청할 수 있습니다.

AWS Glue 데이터 원본을 추가하려면

1. Amazon DataZone 데이터 포털 URL로 이동하여 싱글 사인온 (SSO) 또는 자격 증명을 사용하여 로그인합니다. AWS Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 위치로 로그인한 다음 Open data portal을 선택할 수 있습니다.
2. 상단 탐색 창에서 프로젝트 선택을 선택하고 데이터 소스를 추가할 프로젝트를 선택합니다.
3. 프로젝트의 데이터 탭으로 이동합니다.
4. 왼쪽 탐색 창에서 데이터 소스를 선택한 다음 데이터 원본 만들기를 선택합니다.
5. 다음 필드를 구성합니다.

   - 이름 - 데이터 원본 이름.
   - 설명 — 데이터 소스 설명.
6. 데이터 소스 유형에서 선택합니다 AWS Glue.
7. 환경 선택에서 AWS Glue 테이블을 게시할 환경을 지정합니다.
8. 데이터 선택에서 AWS Glue 데이터베이스를 제공하고 테이블 선택 기준을 입력합니다. 예를 들어 포함을 선택하고 `*corporate` Enter를 선택하면 데이터베이스에는 해당 단어로 끝나는 모든 원본 테이블이 포함됩니다`corporate`.

   드롭다운에서 데이터베이스를 선택하거나 AWS Glue 데이터베이스 이름을 입력할 수 있습니다. 드롭다운에는 게시 데이터베이스와 환경의 구독 데이터베이스라는 두 개의 데이터베이스가 포함됩니다. 환경에서 만들지 않은 데이터베이스의 자산을 가져오려면 드롭다운에서 데이터베이스를 선택하는 대신 데이터베이스 이름을 입력해야 합니다.

   단일 데이터베이스 내의 테이블에 대해 여러 개의 포함 및 제외 규칙을 추가할 수 있습니다. 다른 데이터베이스 추가 버튼을 사용하여 여러 데이터베이스를 추가할 수도 있습니다.

9. 데이터 품질에서 이 데이터 원본의 데이터 품질 활성화를 선택할 수 있습니다. 이렇게 하면 Amazon은 기존 AWS Glue 데이터 품질 출력을 Amazon DataZone 카탈로그로 DataZone 가져옵니다. 기본적으로 Amazon은 AWS Glue로부터 만료 날짜 없이 기존 100개의 최신 품질 보고서를 DataZone 가져옵니다.

   Amazon의 데이터 품질 메트릭은 데이터 소스의 완전성과 정확성을 이해하는 DataZone 데 도움이 됩니다. Amazon은 특정 시점 (예: 비즈니스 데이터 카탈로그 검색) 동안 컨텍스트를 제공하기

위해 AWS Glue에서 이러한 데이터 품질 지표를 DataZone 가져옵니다. 데이터 사용자는 구독한 자산의 데이터 품질 지표가 시간이 지남에 따라 어떻게 변하는지 확인할 수 있습니다. 데이터 생산자는 일정에 따라 AWS Glue 데이터 품질 점수를 수집할 수 있습니다. Amazon DataZone 비즈니스 데이터 카탈로그는 데이터 품질 API를 통해 타사 시스템의 데이터 품질 메트릭을 표시할 수도 있습니다. 자세한 내용은 아마존의 데이터 품질 DataZone단원을 참조하세요.

10. 다음을 선택합니다.
11. 게시 설정의 경우 비즈니스 데이터 카탈로그에서 자산을 즉시 검색할 수 있는지 여부를 선택합니다. 인벤토리에만 추가하는 경우 나중에 구독 조건을 선택하여 비즈니스 데이터 카탈로그에 게시할 수 있습니다. 자세한 정보는 the section called “기존 데이터 소스 관리”을 참조하세요.
12. 자동 비즈니스 이름 생성의 경우 소스에서 자산을 가져올 때 자산에 대한 메타데이터를 자동으로 생성할지 여부를 선택합니다.
13. (선택 사항) 메타데이터 양식의 경우, 자산을 Amazon으로 가져올 때 수집 및 저장되는 메타데이터를 정의하는 양식을 추가합니다 DataZone. 자세한 정보는 the section called “메타데이터 양식을 생성, 편집 또는 삭제합니다.”을 참조하세요.
14. 실행 환경설정에서 데이터 소스 실행 시기를 선택합니다.

    - 일정에 따라 실행 - 데이터 원본을 실행할 날짜 및 시간을 지정합니다.
    - 온디맨드 실행 - 데이터 원본 실행을 수동으로 시작할 수 있습니다.

15. 다음을 선택합니다.
16. 데이터 원본 구성을 검토하고 만들기를 선택합니다.

아마존 Redshift용 아마존 DataZone 데이터 소스 생성 및 실행

DataZoneAmazon에서는 Amazon Redshift 데이터 웨어하우스에서 데이터베이스 테이블 및 뷰의 기술 메타데이터를 가져오기 위해 Amazon Redshift 데이터 소스를 생성할 수 있습니다. Amazon Redshift에 아마존 DataZone 데이터 소스를 추가하려면 소스 데이터 웨어하우스가 Amazon Redshift에 이미 있어야 합니다.

Amazon Redshift 데이터 소스를 생성하고 실행하면 소스 Amazon Redshift 데이터 웨어하우스의 자산을 Amazon 프로젝트 인벤토리에 추가합니다. DataZone Amazon Redshift 데이터 소스를 정해진 일정에 따라 또는 필요에 따라 실행하여 자산의 기술 메타데이터를 생성하거나 업데이트할 수 있습니다. 데이터 소스 실행 중에 프로젝트 인벤토리 자산을 Amazon DataZone 카탈로그에 게시하여 모든 도메인 사용자가 검색할 수 있도록 할 수도 있습니다. 비즈니스 메타데이터를 편집한 후 인벤토리 자산을 게시할 수도 있습니다. 도메인 사용자는 게시된 자산을 검색 및 검색하고 해당 자산에 대한 구독을 요청할 수 있습니다.

Amazon Redshift 데이터 소스를 추가하려면

1. Amazon DataZone 데이터 포털 URL로 이동하여 싱글 사인온 (SSO) 또는 자격 증명을 사용하여 로그인합니다. AWS Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 위치로 로그인한 다음 Open data portal을 선택할 수 있습니다.
2. 상단 탐색 창에서 프로젝트 선택을 선택하고 데이터 소스를 추가할 프로젝트를 선택합니다.
3. 프로젝트의 데이터 탭으로 이동합니다.
4. 왼쪽 탐색 창에서 데이터 소스를 선택한 다음 데이터 원본 만들기를 선택합니다.
5. 다음 필드를 구성합니다.
   - 이름 - 데이터 원본 이름.
   - 설명 — 데이터 소스 설명.
6. 데이터 소스 유형에서 Amazon Redshift를 선택합니다.
7. 환경 선택에서 Amazon Redshift 테이블을 게시할 환경을 지정합니다.
8. 선택한 환경에 따라 DataZone Amazon은 자동으로 Amazon Redshift 자격 증명 및 기타 매개 변수를 환경에서 직접 적용하거나 사용자가 직접 선택할 수 있는 옵션을 제공합니다.
   - 환경의 기본 Amazon Redshift 스키마에서 게시만 허용하는 환경을 선택한 경우 Amazon은 Amazon Redshift 자격 증명과 Amazon Redshift 클러스터 또는 작업 그룹 이름 AWS , 암호, 데이터베이스 이름, 스키마 이름을 비롯한 기타 파라미터를 DataZone 자동으로 적용합니다. 이렇게 자동으로 채워진 매개변수는 편집할 수 없습니다.
   - 데이터를 게시할 수 없는 환경을 선택하면 데이터 원본 생성을 계속할 수 없습니다.
   - 모든 스키마에서 데이터를 게시할 수 있는 환경을 선택하면 해당 환경의 자격 증명 및 기타 Amazon Redshift 파라미터를 사용하거나 자체 자격 증명/파라미터를 입력할 수 있는 옵션이 표시됩니다.
9. 자체 자격 증명을 사용하여 데이터 소스를 생성하기로 선택한 경우 다음 세부 정보를 제공하십시오.
   - Amazon Redshift 자격 증명 제공에서 프로비저닝된 Amazon Redshift 클러스터를 사용할지 아니면 Amazon Redshift 서버리스 작업 공간을 데이터 소스로 사용할지를 선택합니다.
   - 위 단계에서 선택한 항목에 따라 드롭다운 메뉴에서 Amazon Redshift 클러스터 또는 작업 공간을 선택한 다음 AWS Secrets Manager에서 인증에 사용할 암호를 선택합니다. 기존 암호를 선택하거나 새 암호를 생성할 수 있습니다.

- 기존 암호가 드롭다운에 나타나도록 하려면 AWS Secrets Manager의 암호에 다음 태그 (키/값)가 포함되어 있어야 합니다.
  - AmazonDataZoneProject: <projectID>
  - AmazonDataZoneDomain: <domainID>

  새 암호를 만들기로 선택하면 암호에 위에서 참조한 태그가 자동으로 지정되므로 추가 단계가 필요하지 않습니다. 자세한 내용은 데이터베이스 자격 증명 저장을 참조하십시오. AWS Secrets Manager

  데이터 소스 생성을 위해 제공된 AWS 암호의 Amazon Redshift 사용자는 게시할 테이블에 대한 SELECT 권한을 가지고 있어야 합니다. Amazon이 DataZone 귀하를 대신하여 구독 (액세스) 을 관리하도록 하려면 AWS 시크릿의 데이터베이스 사용자에게도 다음과 같은 권한이 있어야 합니다.
  - `CREATE DATASHARE`
  - `ALTER DATASHARE`
  - `DROP DATASHARE`

10. 데이터 선택에서 Amazon Redshift 데이터베이스, 스키마를 제공하고 테이블 또는 뷰 선택 기준을 입력합니다. 예를 들어 Include를 선택하고 **`*corporate`** Enter를 선택하면 해당 단어로 **`corporate`** 끝나는 모든 소스 테이블이 자산에 포함됩니다.

    단일 데이터베이스 내의 테이블에 대해 여러 개의 포함 규칙을 추가할 수 있습니다. 다른 데이터베이스 추가 버튼을 사용하여 여러 데이터베이스를 추가할 수도 있습니다.
11. 다음을 선택합니다.
12. 게시 설정의 경우 데이터 카탈로그에서 자산을 즉시 검색할 수 있는지 여부를 선택합니다. 인벤토리에만 추가하는 경우 나중에 구독 조건을 선택하여 비즈니스 데이터 카탈로그에 게시할 수 있습니다. 자세한 정보는 the section called “기존 데이터 소스 관리”을 참조하세요.
13. 자동 비즈니스 이름 생성의 경우 원본에서 게시되고 업데이트되는 자산의 메타데이터를 자동으로 생성할지 여부를 선택합니다.
14. (선택 사항) 메타데이터 양식의 경우, 자산을 Amazon으로 가져올 때 수집 및 저장되는 메타데이터를 정의하는 양식을 추가합니다 DataZone. 자세한 정보는 the section called “메타데이터 양식을 생성, 편집 또는 삭제합니다.”을 참조하세요.
15. 실행 환경설정에서 데이터 소스 실행 시기를 선택합니다.
    - 일정에 따라 실행 - 데이터 원본을 실행할 날짜 및 시간을 지정합니다.
    - 온디맨드 실행 - 데이터 원본 실행을 수동으로 시작할 수 있습니다.

16. 다음을 선택합니다.
17. 데이터 원본 구성을 검토하고 만들기를 선택합니다.

기존 Amazon DataZone 데이터 소스 관리

Amazon DataZone 데이터 소스를 생성한 후 언제든지 수정하여 소스 세부 정보 또는 데이터 선택 기준을 변경할 수 있습니다. 더 이상 필요하지 않은 데이터 소스는 삭제할 수 있습니다.

이 단계를 완료하려면 AmazonDataZoneFullAccess AWS 관리형 정책이 연결되어 있어야 합니다. 자세한 정보는 the section called “AWS 관리형 정책”을 참조하세요.

주제

- 데이터 원본 편집
- 데이터 원본 삭제

데이터 원본 편집

Amazon DataZone 데이터 소스를 편집하여 테이블 선택 기준 추가, 제거 또는 변경을 비롯한 데이터 선택 설정을 수정할 수 있습니다. 데이터베이스를 추가 및 제거할 수도 있습니다. 데이터 원본 유형이나 데이터 원본이 게시된 환경을 변경할 수 없습니다.

데이터 원본을 편집하려면

1. Amazon DataZone 데이터 포털 URL로 이동하여 싱글 사인온 (SSO) 또는 자격 증명을 사용하여 로그인합니다. AWS Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 위치로 로그인한 다음 Open data portal을 선택할 수 있습니다.
2. 상단 탐색 창에서 프로젝트 선택을 선택하고 데이터 소스가 속한 프로젝트를 선택합니다.
3. 프로젝트의 데이터 탭으로 이동합니다.
4. 왼쪽 탐색 창에서 데이터 소스를 선택한 다음 수정하려는 데이터 원본을 선택합니다.
5. 데이터 원본 정의 탭으로 이동한 다음 편집을 선택합니다.
6. 데이터 소스 정의를 변경합니다. 데이터 원본 세부 정보를 업데이트하고 데이터 선택 기준을 변경할 수 있습니다.
7. 변경 작업을 마치면 저장을 선택합니다.

데이터 원본 삭제

Amazon DataZone 데이터 소스가 더 이상 필요하지 않은 경우 영구적으로 제거할 수 있습니다. 데이터 소스를 삭제한 후에도 해당 데이터 소스에서 생성된 모든 자산을 카탈로그에서 계속 사용할 수 있으며 사용자는 계속 구독할 수 있습니다. 하지만 해당 에셋은 소스로부터 업데이트를 더 이상 받지 않게 됩니다. 종속 자산을 삭제하기 전에 먼저 다른 데이터 소스로 이동하는 것이 좋습니다.

> **Note**
>
> 삭제하려면 먼저 데이터 소스의 모든 주문 처리를 제거해야 합니다. 자세한 정보는 Amazon에서 데이터 검색, 구독 및 사용 DataZone을 참조하세요.

데이터 소스를 삭제하기

1. 프로젝트의 데이터 탭에 있는 왼쪽 탐색 창에서 데이터 소스를 선택합니다.
2. 삭제하려는 데이터 원본을 선택합니다.
3. 작업, 데이터 원본 삭제를 선택하고 삭제를 확인합니다.

프로젝트 인벤토리에서 자산을 Amazon DataZone 카탈로그에 게시합니다.

프로젝트 인벤토리의 Amazon DataZone 자산 및 메타데이터를 Amazon DataZone 카탈로그에 게시할 수 있습니다. 가장 최신 버전의 자산만 카탈로그에 게시할 수 있습니다.

자산을 카탈로그에 게시할 때는 다음 사항을 고려하십시오.

- 에셋을 카탈로그에 게시하려면 해당 프로젝트의 소유자 또는 기여자여야 합니다.
- Amazon Redshift 자산의 경우, 아마존에서 Redshift 테이블 및 뷰에 대한 액세스를 관리하려면 게시자 및 구독자 클러스터 모두와 연결된 Amazon Redshift 클러스터가 Amazon Redshift 데이터 공유에 대한 모든 요구 사항을 충족하는지 확인하십시오. DataZone Amazon Redshift의 데이터 공유 개념을 참조하십시오.
- Amazon은 AWS Glue Data Catalog 및 Amazon Redshift에서 게시된 자산에 대한 액세스 DataZone 관리만 지원합니다. Amazon S3 객체와 같은 기타 모든 자산의 경우 DataZone Amazon은 승인된 구독자의 액세스를 관리하지 않습니다. 이러한 비관리형 자산을 구독하는 경우 다음 메시지와 함께 알림을 받게 됩니다.

```
Subscription approval does not provide access to data. Subscription
grants on this asset are not managed by Amazon DataZone. For more
information or help, reach out to your administrator.
```

자산 게시

데이터 원본을 만들 때 데이터 카탈로그에서 자산을 즉시 검색할 수 있도록 설정하지 않은 경우 다음 단계를 수행하여 나중에 게시하십시오.

자산을 게시하려면

1. Amazon DataZone 데이터 포털 URL로 이동하여 싱글 사인온 (SSO) 또는 자격 증명을 사용하여 로그인합니다. AWS Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 위치로 로그인한 다음 Open data portal을 선택할 수 있습니다.
2. 상단 탐색 창에서 프로젝트 선택을 선택하고 자산이 속한 프로젝트를 선택합니다.
3. 프로젝트의 데이터 탭으로 이동합니다.
4. 왼쪽 탐색 창에서 인벤토리 데이터를 선택한 다음 게시하려는 자산을 선택합니다.

   > **Note**
   >
   > 기본적으로 모든 자산에는 구독 승인이 필요합니다. 즉, 데이터 소유자가 자산에 대한 모든 구독 요청을 승인해야 합니다. 자산을 게시하기 전에 이 설정을 변경하려면 자산 세부 정보를 열고 구독 승인 옆의 편집을 선택합니다. 나중에 자산을 수정하고 다시 게시하여 이 설정을 변경할 수 있습니다.

5. 에셋 게시를 선택합니다. 자산은 카탈로그에 직접 게시됩니다.

   승인 요구 사항을 수정하는 등 자산을 변경하는 경우 재게시를 선택하여 카탈로그에 업데이트를 게시할 수 있습니다.

인벤토리 관리 및 자산 큐레이션

DataZone Amazon을 사용하여 데이터를 카탈로그화하려면 먼저 데이터 (자산) 를 프로젝트 인벤토리로 Amazon에 가져와야 DataZone 합니다. 특정 프로젝트에 대한 인벤토리를 생성하면 해당 프로젝트 구성원만 자산을 검색할 수 있습니다.

프로젝트 인벤토리에 에셋이 생성되면 해당 메타데이터를 큐레이션할 수 있습니다. 예를 들어 에셋의 이름, 설명을 편집하거나 Read Me. 자산을 편집할 때마다 자산의 새 버전이 만들어집니다. 자산 세부 정보 페이지의 기록 탭을 사용하여 모든 자산 버전을 볼 수 있습니다.

Read Me 섹션을 편집하고 자산에 대한 풍부한 설명을 추가할 수 있습니다. Read Me 섹션은 마크다운을 지원하므로 필요에 따라 설명 형식을 지정하고 소비자에게 자산에 대한 주요 정보를 설명할 수 있습니다.

사용 가능한 양식을 작성하여 자산 수준에서 용어집 용어를 추가할 수 있습니다.

스키마를 조정하려면 열을 검토하고, 비즈니스 이름, 설명을 추가하고, 열 수준에서 용어집 용어를 추가할 수 있습니다.

데이터 소스를 만들 때 자동 메타데이터 생성이 활성화된 경우 자산 및 열의 비즈니스 이름을 개별적으로 또는 한 번에 검토 및 승인 또는 거부할 수 있습니다.

구독 조건을 편집하여 자산에 대한 승인이 필요한지 여부를 지정할 수도 있습니다.

Amazon의 메타데이터 양식을 DataZone 사용하면 사용자 정의 속성 (예: 판매 지역, 판매 연도, 판매 분기) 을 추가하여 데이터 자산의 메타데이터 모델을 확장할 수 있습니다. 자산 유형에 첨부된 메타데이터 양식은 해당 자산 유형에서 생성된 모든 자산에 적용됩니다. 또한 데이터 소스 실행의 일부로 또는 만든 후에 개별 자산에 메타데이터 양식을 추가할 수 있습니다. 새 양식을 만들려면 을 참조하십시오the section called “메타데이터 양식을 생성, 편집 또는 삭제합니다.”.

자산의 메타데이터를 업데이트하려면 자산이 속한 프로젝트의 소유자 또는 기여자여야 합니다.

자산의 메타데이터를 업데이트하려면

1. Amazon DataZone 데이터 포털 URL로 이동하여 싱글 사인온 (SSO) 또는 자격 증명을 사용하여 로그인합니다. AWS Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 위치로 로그인한 다음 Open data portal을 선택할 수 있습니다.
2. 상단 탐색 창에서 프로젝트 선택을 선택하고 메타데이터를 업데이트하려는 자산이 포함된 프로젝트를 선택합니다.
3. 프로젝트의 데이터 탭으로 이동합니다.
4. 왼쪽 탐색 창에서 인벤토리 데이터를 선택한 다음 메타데이터를 업데이트하려는 자산의 이름을 선택합니다.
5. 자산 세부 정보 페이지의 메타데이터 양식에서 편집을 선택하고 필요에 따라 기존 양식을 편집합니다. 자산에 추가 메타데이터 양식을 첨부할 수도 있습니다. 자세한 정보는 the section called “자산에 추가 메타데이터 양식을 첨부합니다.”을 참조하세요.

6. 업데이트를 완료하면 양식 저장을 선택합니다.

   양식을 저장하면 Amazon에서 자산의 새 인벤토리 버전을 DataZone 생성합니다. 업데이트된 버전을 카탈로그에 게시하려면 자산 재게시를 선택합니다.

자산에 추가 메타데이터 양식을 첨부합니다.

기본적으로 도메인에 연결된 메타데이터 양식은 해당 도메인에 게시된 모든 자산에 첨부됩니다. 데이터 게시자는 추가 컨텍스트를 제공하기 위해 추가 메타데이터 양식을 개별 자산에 연결할 수 있습니다.

자산에 추가 메타데이터 양식을 첨부하려면

1. Amazon DataZone 데이터 포털 URL로 이동하여 싱글 사인온 (SSO) 또는 자격 증명을 사용하여 로그인합니다. AWS Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 위치로 로그인한 다음 Open data portal을 선택할 수 있습니다.
2. 상단 탐색 창에서 프로젝트 선택을 선택하고 메타데이터를 추가하려는 자산이 포함된 프로젝트를 선택합니다.
3. 프로젝트의 데이터 탭으로 이동합니다.
4. 왼쪽 탐색 창에서 인벤토리 데이터를 선택한 다음 메타데이터를 추가하려는 자산의 이름을 선택합니다.
5. 자산 세부 정보 페이지의 메타데이터 양식에서 양식 추가를 선택합니다.
6. 자산에 추가할 양식을 선택한 다음 양식 추가를 선택합니다.
7. 각 메타데이터 필드에 값을 입력한 다음 양식 저장을 선택합니다.

   양식을 저장하면 Amazon에서 자산의 새 인벤토리 버전을 DataZone 생성합니다. 업데이트된 버전을 카탈로그에 게시하려면 자산 재게시를 선택합니다.

큐레이션 후 자산을 카탈로그에 게시하십시오.

자산 큐레이션에 만족하면 데이터 소유자는 Amazon DataZone 카탈로그에 자산 버전을 게시하여 모든 도메인 사용자가 검색할 수 있도록 할 수 있습니다. 자산에는 인벤토리 버전과 게시된 버전이 표시됩니다. 검색 카탈로그에는 가장 최근에 게시된 버전만 표시됩니다. 게시 후 메타데이터가 업데이트되면 새 인벤토리 버전을 카탈로그에 게시할 수 있게 됩니다.

자산을 수동으로 생성하십시오.

Amazon에서 자산은 단일 물리적 데이터 객체 (예: 테이블 DataZone, 대시보드, 파일) 또는 가상 데이터 객체 (예: 뷰) 를 제공하는 엔티티입니다. 자세한 정보는 아마존 DataZone 용어 및 개념을 참조하세요. 자산을 수동으로 게시하는 것은 일회성 작업입니다. 에셋의 실행 일정을 지정하지 않으므로 소스가 변경되어도 자동으로 업데이트되지 않습니다.

프로젝트를 통해 자산을 수동으로 만들려면 해당 프로젝트의 소유자 또는 기여자여야 합니다.

에셋을 수동으로 만들려면

1. Amazon DataZone 데이터 포털 URL로 이동하여 싱글 사인온 (SSO) 또는 자격 증명을 사용하여 로그인합니다. AWS Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 위치로 로그인한 다음 Open data portal을 선택할 수 있습니다.
2. 상단 탐색 창에서 프로젝트 선택을 선택하고 자산을 생성할 프로젝트를 선택합니다.
3. 프로젝트의 데이터 탭으로 이동합니다.
4. 왼쪽 탐색 창에서 데이터 소스를 선택한 다음 데이터 자산 만들기를 선택합니다.
5. 자산 세부 정보에서 다음 설정을 구성하십시오.
   - 자산 유형 - 자산 유형.
   - 이름 — 자산의 이름.
   - 설명 — 자산에 대한 설명.
6. S3 위치의 경우 원본 S3 버킷의 Amazon 리소스 이름 (ARN) 을 입력합니다.

   선택적으로 S3 액세스 포인트를 입력합니다. 자세한 내용을 알아보려면 Amazon S3 액세스 지점을 사용한 데이터 액세스 관리를 참조하십시오.
7. 게시 설정의 경우 카탈로그에서 자산을 즉시 검색할 수 있는지 여부를 선택합니다. 인벤토리에만 추가하는 경우 나중에 구독 조건을 선택하여 카탈로그에 게시할 수 있습니다.
8. 생성을 선택합니다.

   자산이 생성되면 카탈로그에 활성 자산으로 직접 게시되거나 게시하기로 결정할 때까지 인벤토리에 저장됩니다.

Amazon DataZone 카탈로그에서 에셋 게시 취소

카탈로그에서 Amazon DataZone 자산을 게시 취소하면 글로벌 검색 결과에 해당 자산이 더 이상 표시되지 않습니다. 신규 사용자는 카탈로그에서 자산 목록을 찾거나 구독할 수 없지만 기존 구독은 모두 동일하게 유지됩니다.

에셋 게시를 취소하려면 에셋이 속한 프로젝트의 소유자 또는 기여자여야 합니다.

에셋 게시 취소하기

1. Amazon DataZone 데이터 포털 URL로 이동하여 싱글 사인온 (SSO) 또는 자격 증명을 사용하여 로그인합니다. AWS Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 위치로 로그인한 다음 Open data portal을 선택할 수 있습니다.
2. 상단 탐색 창에서 프로젝트 선택을 선택하고 자산이 속한 프로젝트를 선택합니다.
3. 프로젝트의 데이터 탭으로 이동합니다.
4. 왼쪽 탐색 창에서 게시된 데이터를 선택합니다.
5. 게시된 자산 목록에서 자산을 찾은 다음 게시 취소를 선택합니다.

   자산이 카탈로그에서 제거됩니다. 게시를 선택하여 언제든지 자산을 다시 게시할 수 있습니다.

아마존 DataZone 에셋 삭제

DataZoneAmazon에서 더 이상 필요하지 않은 자산은 영구 삭제할 수 있습니다. 자산을 삭제하는 것은 카탈로그에서 자산을 게시 취소하는 것과 다릅니다. 카탈로그에서 자산 및 관련 목록을 삭제하여 검색 결과에 표시되지 않도록 할 수 있습니다. 자산 목록을 삭제하려면 먼저 모든 구독을 취소해야 합니다.

자산을 삭제하려면 해당 자산이 속한 프로젝트의 소유자 또는 기여자여야 합니다.

> **Note**
>
> 자산 목록을 삭제하려면 먼저 자산에 대한 기존 구독을 모두 취소해야 합니다. 기존 구독자가 있는 자산 목록은 삭제할 수 없습니다.

자산을 삭제하려면

1. Amazon DataZone 데이터 포털 URL로 이동하여 싱글 사인온 (SSO) 또는 자격 증명을 사용하여 로그인합니다. AWS Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 위치로 로그인한 다음 Open data portal을 선택할 수 있습니다.
2. 상단 탐색 창에서 프로젝트 선택을 선택하고 삭제하려는 자산이 포함된 프로젝트를 선택합니다.
3. 프로젝트의 데이터 탭으로 이동합니다.
4. 왼쪽 탐색 창에서 게시된 데이터를 선택한 다음 삭제하려는 자산을 찾아 선택합니다. 그러면 자산 세부 정보 페이지가 열립니다.
5. 작업, 삭제를 선택하고 삭제를 확인합니다.

   일단 삭제된 자산은 더 이상 볼 수 없으며 사용자는 구독할 수 없습니다.

Amazon에서 수동으로 데이터 소스 실행 시작 DataZone

데이터 소스를 실행하면 Amazon은 소스에서 모든 신규 또는 수정된 메타데이터를 DataZone 가져와서 인벤토리의 관련 자산을 업데이트합니다. DataZoneAmazon에 데이터 소스를 추가할 때 소스의 실행 기본 설정을 지정하여 소스가 일정에 따라 실행되는지 아니면 온디맨드 방식으로 실행되는지를 정의합니다. 소스가 온디맨드로 실행되는 경우 데이터 소스 실행을 수동으로 시작해야 합니다.

소스가 일정에 따라 실행되더라도 언제든지 수동으로 실행할 수 있습니다. 자산에 비즈니스 메타데이터를 추가한 후 모든 도메인 사용자가 해당 자산을 검색할 수 있도록 자산을 선택하고 Amazon DataZone 카탈로그에 게시할 수 있습니다. 게시된 자산만 다른 도메인 사용자가 검색할 수 있습니다.

데이터 원본을 수동으로 실행하려면

1. Amazon DataZone 데이터 포털 URL로 이동하여 싱글 사인온 (SSO) 또는 자격 증명을 사용하여 로그인합니다. AWS Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 위치로 로그인한 다음 Open data portal을 선택할 수 있습니다.
2. 상단 탐색 창에서 프로젝트 선택을 선택하고 데이터 소스가 속한 프로젝트를 선택합니다.
3. 프로젝트의 데이터 탭으로 이동합니다.
4. 왼쪽 탐색 창에서 데이터 소스를 선택한 다음 실행하려는 데이터 원본을 찾아 선택합니다. 그러면 데이터 원본 세부정보 페이지가 열립니다.
5. [Run on demand] 를 선택합니다.

Amazon이 소스의 최신 Running 데이터로 자산 메타데이터를 DataZone 업데이트하면 데이터 소스 상태가 로 변경됩니다. 데이터 소스 실행 탭에서 실행 상태를 모니터링할 수 있습니다.

아마존의 자산 수정 DataZone

Amazon은 자산의 비즈니스 또는 기술 메타데이터를 편집할 때 자산의 수정 내용을 DataZone 늘립니다. 이러한 편집에는 자산 이름, 설명, 용어집 용어, 열 이름, 메타데이터 양식 및 메타데이터 양식 필드 값의 수정이 포함됩니다. 이러한 변경은 수동 편집, 데이터 원본 작업 실행 또는 API 조작으로 인해 발생할 수 있습니다. Amazon은 자산을 편집할 때마다 새 자산 수정 버전을 DataZone 자동으로 생성합니다.

자산을 업데이트하고 새 수정본을 생성한 후에는 새 수정 버전을 카탈로그에 게시해야 업데이트되어 구독자가 이용할 수 있습니다. 자세한 정보는 the section called “프로젝트 인벤토리에서 카탈로그에 자산을 게시하십시오.”을 참조하세요. 가장 최신 버전의 자산만 카탈로그에 게시할 수 있습니다.

자산의 이전 수정 버전을 보려면

1. Amazon DataZone 데이터 포털 URL로 이동하여 싱글 사인온 (SSO) 또는 자격 증명을 사용하여 로그인합니다. AWS Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 위치로 로그인한 다음 Open data portal을 선택할 수 있습니다.
2. 상단 탐색 창에서 프로젝트 선택을 선택하고 자산이 포함된 프로젝트를 선택합니다.
3. 프로젝트의 데이터 탭으로 이동한 다음 에셋을 찾아 선택합니다. 그러면 에셋 세부정보 페이지가 열립니다.
4. 에셋의 과거 수정 목록이 표시된 기록 탭으로 이동합니다.

아마존의 데이터 품질 DataZone

Amazon의 데이터 품질 메트릭은 데이터 소스의 완전성, 적시성, 정확성과 같은 다양한 품질 메트릭을 이해하는 DataZone 데 도움이 됩니다. DataZoneAmazon은 AWS Glue Data Quality와 통합하고 타사 데이터 품질 솔루션의 데이터 품질 메트릭을 통합하는 API를 제공합니다. 데이터 사용자는 구독한 자산의 데이터 품질 지표가 시간이 지남에 따라 어떻게 변하는지 확인할 수 있습니다. 데이터 품질 규칙을 작성하고 실행하려면 AWS Glue data quality 같은 원하는 데이터 품질 도구를 사용할 수 있습니다. DataZoneAmazon의 데이터 품질 지표를 통해 데이터 소비자는 자산 및 열에 대한 데이터 품질 점수를 시각화하여 의사 결정에 사용하는 데이터에 대한 신뢰를 구축할 수 있습니다.

사전 요구 사항 및 IAM 역할 변경

DataZoneAmazon의 AWS 관리형 정책을 사용하는 경우 추가 구성 단계가 없으며 이러한 관리형 정책은 데이터 품질을 지원하도록 자동으로 업데이트됩니다. 지원되는 서비스와 상호 운용하는 데 필요한 권한을 DataZone Amazon에 부여하는 역할에 대해 자체 정책을 사용하는 경우, 이러한 역할에 연결된 정책을 업데이트하여 에서 AWS Glue 데이터 품질 정보를 읽을 수 있도록 지원하고 AWS 관리형 정책: AmazonDataZoneGlueManageAccessRolePolicy 및 에서 시계열 API에 대한 지원을 활성화해야 합니다. AWS 관리형 정책: AmazonDataZoneDomainExecutionRolePolicy AWS 관리형 정책: AmazonDataZoneFullUserAccess

AWS Glue 에셋의 데이터 품질 활성화

Amazon은 특정 시점 (예: 비즈니스 데이터 카탈로그 검색) 동안 컨텍스트를 제공하기 위해 AWS Glue에서 데이터 품질 지표를 DataZone 가져옵니다. 데이터 사용자는 구독한 자산의 데이터 품질 지표가 시간이 지남에 따라 어떻게 변하는지 확인할 수 있습니다. 데이터 생산자는 일정에 따라 AWS Glue 데이터 품질 점수를 수집할 수 있습니다. Amazon DataZone 비즈니스 데이터 카탈로그는 데이터 품질 API를 통해 타사 시스템의 데이터 품질 메트릭을 표시할 수도 있습니다. 자세한 내용은 AWS Glue 데이터 품질 및 데이터 카탈로그의 AWS Glue 데이터 품질 시작하기를 참조하십시오.

다음과 같은 방법으로 Amazon DataZone 자산에 대한 데이터 품질 메트릭을 활성화할 수 있습니다.

- 데이터 포털 또는 Amazon DataZone API를 사용하면 Amazon 데이터 포털을 통해 Glue 데이터 소스를 새로 만들거나 기존 AWS Glue 데이터 소스를 편집할 때 AWS Glue DataZone 데이터 소스의 데이터 품질을 활성화할 수 있습니다.

  포털을 통해 데이터 소스의 데이터 품질을 활성화하는 방법에 대한 자세한 내용은 다음을 위한 Amazon DataZone 데이터 소스 생성 및 실행 AWS Glue Data Catalog 및 기존 Amazon DataZone 데이터 소스 관리 을 참조하십시오.

  > **Note**
  >
  > Data Portal을 사용하여 AWS Glue 인벤토리 자산에 대해서만 데이터 품질을 활성화할 수 있습니다. 이번 Amazon 릴리스에서는 데이터 포털을 통한 Amazon Redshift 또는 사용자 지정 유형 자산의 데이터 품질 DataZone 활성화가 지원되지 않습니다.

  또한 API를 사용하여 신규 또는 기존 데이터 소스의 데이터 품질을 활성화할 수 있습니다. or를 UpdateDataSource호출하고 `autoImportDataQualityResult` 매개변수를 'True'로 CreateDataSource설정하여 이 작업을 수행할 수 있습니다.

데이터 품질이 활성화되면 필요에 따라 또는 일정에 따라 데이터 원본을 실행할 수 있습니다. 각 실행은 자산당 최대 100개의 지표를 가져올 수 있습니다. 데이터 품질을 위해 데이터 소스를 사용하는 경우 수동으로 양식을 만들거나 지표를 추가할 필요가 없습니다. 자산이 게시되면 데이터 품질 양식에 적용된 업데이트 (기록 규칙당 최대 30개의 데이터 포인트) 가 소비자를 위한 목록에 반영됩니다. 이후 자산에 지표가 새로 추가될 때마다 자동으로 목록에 추가됩니다. 소비자가 최신 점수를 볼 수 있도록 자산을 다시 게시할 필요는 없습니다.

사용자 지정 자산 유형에 대한 데이터 품질 지원

Amazon DataZone API를 사용하여 모든 사용자 지정 유형 자산의 데이터 품질을 활성화할 수 있습니다. 자세한 내용은 다음을 참조하십시오.

- PostTimeSeriesDataPoints
- ListTimeSeriesDataPoints
- GetTimeSeriesDataPoint
- DeleteTimeSeriesDataPoints

다음 단계는 API 또는 CLI를 사용하여 Amazon 자산에 대한 타사 메트릭을 가져오는 예를 제공합니다. DataZone

1. 다음과 같이 `PostTimeSeriesDataPoints` API를 호출합니다.

```
aws datazone post-time-series-data-points  \
--cli-input-json file://createTimeSeriesPayload.json \
```

다음 페이로드와 함께:

```
{
"domainIdentifier": "dzd_bqqlk3nz21zp2f",
"entityIdentifier": "4nwl5ew0dsu27b",
"entityType": "ASSET",
"forms": [
{
```

```
"content": "{\n \"evaluationsCount\" : 11,\n \"evaluations\" : [ {\n \"description
\" : \"IsComplete \\\"Id\\\"\",\n \"details\" : {\n \"STATISTIC_NAME\" :
 \"Completeness\",\n \"COLUMN_NAME\" : \"Id\"\n },\n \"status\" : \"PASS\"\n },
 {\n \"description\" : \"Uniqueness \\\"Id\\\" > 0.95\",\n \"details\" : {\n
 \"STATISTIC_NAME\" : \"Uniqueness\",\n \"COLUMN_NAME\" : \"Id\"\n },\n \"status
\" : \"PASS\"\n }, {\n \"description\" : \"ColumnLength \\\"Id\\\" = 18\",\n
 \"details\" : {\n \"STATISTIC_NAME\" : \"MinimumLength,MaximumLength\",\n
 \"COLUMN_NAME\" : \"Id,Id\"\n },\n \"status\" : \"PASS\"\n }, {\n \"description
\" : \"IsComplete \\\"IsDeleted\\\"\",\n \"details\" : {\n \"STATISTIC_NAME\" :
 \"Completeness\",\n \"COLUMN_NAME\" : \"IsDeleted\"\n },\n \"status\" : \"PASS
\"\n }, {\n \"description\" : \"Completeness \\\"Type\\\" >= 0.59\",\n \"details
\" : {\n \"STATISTIC_NAME\" : \"Completeness\",\n \"COLUMN_NAME\" : \"Type\"\n },
\n \"status\" : \"PASS\"\n }, {\n \"description\" : \"ColumnValues \\\"Type\
\\" in [\\\"Customer - Direct\\\",\\\"Customer - Channel\\\"] with threshold
 >= 0.8\",\n \"details\" : {\n \"STATISTIC_NAME\" : \"\",\n \"COLUMN_NAME\" :
 \"\"\n },\n \"status\" : \"PASS\"\n }, {\n \"description\" : \"ColumnLength \\
\"Type\\\" <= 18\",\n \"details\" : {\n \"STATISTIC_NAME\" : \"MaximumLength\",\n
 \"COLUMN_NAME\" : \"Type\"\n },\n \"status\" : \"PASS\"\n }, {\n \"description
\" : \"ColumnLength \\\"ParentId\\\" <= 18\",\n \"details\" : {\n \"STATISTIC_NAME
\" : \"MaximumLength\",\n \"COLUMN_NAME\" : \"ParentId\"\n },\n \"status\" :
 \"PASS\"\n }, {\n \"description\" : \"Completeness \\\"AnnualRevenue\\\" >=
 0.28\",\n \"details\" : {\n \"STATISTIC_NAME\" : \"Completeness\",\n \"COLUMN_NAME
\" : \"AnnualRevenue\"\n },\n \"status\" : \"PASS\"\n }, {\n \"description
\" : \"StandardDeviation \\\"AnnualRevenue\\\" between 1658483123.39 and
 1833060294.28\",\n \"details\" : {\n \"STATISTIC_NAME\" : \"StandardDeviation
\",\n \"COLUMN_NAME\" : \"AnnualRevenue\"\n },\n \"status\" : \"PASS\"\n }, {\n
 \"description\" : \"ColumnValues \\\"AnnualRevenue\\\" between 29999999 and
 5600000001\",\n \"details\" : {\n \"STATISTIC_NAME\" : \"Minimum,Maximum\",\n
 \"COLUMN_NAME\" : \"AnnualRevenue,AnnualRevenue\"\n },\n \"status\" : \"PASS
\"\n } ],\n \"passingPercentage\" : 1.0\n}",
"formName": "GREAT_EXPECTATION_NEW",
"typeIdentifier": "amazon.datazone.DataQualityResultFormType",
"timestamp": 1608969556
}
]
}
```

2. 다음과 같이 DeleteTimeSeriesDataPoints API를 호출합니다.

```
aws datazone delete-time-series-data-points\
--domain-identifier dzd_bqqlk3nz21zp2f \
--entity-identifier dzd_bqqlk3nz21zp2f \
```

```
--entity-type ASSET \
--form-name rulesET1 \
```

머신 러닝 및 제너레이티브 AI 사용

> **Note**
>
> Amazon Bedrock 제공: 자동 악용 탐지 AWS 기능을 구현합니다. Amazon의 설명 기능에 대한 AI 권장 사항은 Amazon DataZone Bedrock을 기반으로 하기 때문에 사용자는 Amazon Bedrock에 구현된 제어 기능을 상속받아 AI의 안전, 보안 및 책임감 있는 사용을 강화합니다.

DataZoneAmazon의 최신 릴리스에서는 설명 기능에 대한 AI 권장 사항을 사용하여 데이터 검색 및 카탈로그 작성을 자동화할 수 있습니다. Amazon의 제너레이티브 AI 및 기계 학습 지원을 통해 자산 및 열에 대한 설명이 DataZone 생성됩니다. 이러한 설명을 사용하여 데이터에 비즈니스 컨텍스트를 추가하고 데이터 세트에 대한 분석을 권장하여 데이터 검색 결과를 높일 수 있습니다.

Amazon Bedrock의 대규모 언어 모델을 기반으로 하는 Amazon의 데이터 자산 설명에 대한 AI 권장 사항은 데이터를 이해하고 쉽게 검색할 수 있도록 DataZone 도와줍니다. 또한 AI 권장 사항은 데이터세트에 가장 적합한 분석 애플리케이션을 제안합니다. 자동 생성된 설명은 수동 문서화 작업을 줄이고 적절한 데이터 사용을 권장함으로써 데이터의 신뢰성을 높이고 중요한 데이터를 간과하는 것을 최소화하여 정보에 입각한 의사 결정을 가속화하는 데 도움이 될 수 있습니다.

> **Important**
>
> 현재 Amazon DataZone 릴리스에서는 설명에 대한 AI 권장 사항 기능이 다음 지역에서만 지원됩니다.
>
> - 미국 동부(버지니아 북부)
> - 미국 서부(오리건)
> - 유럽(프랑크푸르트)
> - 아시아 태평양(도쿄)

다음 절차는 Amazon의 설명에 대한 AI 권장 사항을 생성하는 방법을 설명합니다 DataZone.

1. Amazon DataZone 데이터 포털 URL로 이동한 다음 싱글 사인온 (SSO) 또는 자격 증명을 사용하여 로그인합니다. AWS Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 위치로 로그인한 다음 Open data portal을 선택합니다.
2. 상단 탐색 창에서 프로젝트 선택을 선택한 다음 설명에 대한 AI 추천을 생성하려는 자산이 포함된 프로젝트를 선택합니다.
3. 프로젝트의 데이터 탭으로 이동합니다.
4. 왼쪽 탐색 창에서 Inventory data를 선택한 다음, 자산에 대한 설명에 대한 AI 추천을 생성하려는 자산의 이름을 선택합니다.
5. 자산의 세부정보 페이지의 비즈니스 메타데이터 탭에서 설명 생성을 선택합니다.
6. 설명이 생성되면 설명을 편집, 수락 또는 거부할 수 있습니다. 데이터 자산에 대해 자동으로 생성된 각 메타데이터 설명 옆에 녹색 아이콘이 표시됩니다. 비즈니스 메타데이터 탭에서 자동으로 생성된 요약 옆에 있는 녹색 아이콘을 선택한 다음 편집, 수락 또는 거부를 선택하여 생성된 설명을 처리할 수 있습니다. 또한 비즈니스 메타데이터 탭을 선택할 때 페이지 상단에 표시되는 옵션을 모두 수락 또는 모두 거부를 선택하여 자동으로 생성된 모든 설명에 대해 선택한 작업을 수행할 수 있습니다.

   또는 스키마 탭을 선택한 다음 한 번에 하나의 열 설명에 녹색 아이콘을 선택한 다음 수락 또는 거부를 선택하여 자동으로 생성된 설명을 개별적으로 처리할 수 있습니다. 스키마 탭에서 모두 수락 또는 모두 거부를 선택하여 자동으로 생성된 모든 설명에 대해 선택한 작업을 수행할 수도 있습니다.
7. 생성된 설명과 함께 자산을 카탈로그에 게시하려면 자산 게시를 선택한 다음 자산 게시 팝업 창에서 자산 게시를 다시 선택하여 이 작업을 확인합니다.

> **Note**
>
> 자산에 대해 생성된 설명을 수락하거나 거부하지 않고 이 자산을 게시하면 검토되지 않은 자동 생성 메타데이터는 게시된 데이터 자산에 포함되지 않습니다.

Amazon에서 데이터 검색, 구독 및 사용 DataZone

DataZoneAmazon에서는 자산이 도메인에 게시되면 구독자가 해당 자산을 검색하고 구독을 요청할 수 있습니다. 구독 프로세스는 구독자가 카탈로그를 검색하고 탐색하여 원하는 자산을 찾는 것으로 시작됩니다. Amazon DataZone 포털에서 사유 및 요청 사유가 포함된 구독 요청을 제출하여 자산을 구독하기로 선택합니다. 그런 다음 게시 계약에 정의된 대로 구독 승인자가 액세스 요청을 검토합니다. 요청을 승인하거나 거부할 수 있습니다.

구독이 승인되면 구독자가 자산에 쉽게 액세스할 수 있도록 주문 처리 프로세스가 시작됩니다. 자산 액세스 제어 및 처리에는 두 가지 기본 모드가 있습니다. 하나는 Amazon에서 DataZone 관리하는 자산용이고 다른 하나는 Amazon에서 관리하지 않는 자산용입니다. DataZone

- 관리 자산 — Amazon은 테이블, Amazon Redshift AWS Glue 테이블 및 뷰와 같은 관리 자산에 대한 주문 처리 및 권한을 관리할 DataZone 수 있습니다.
- 비관리 자산 — Amazon은 사용자의 활동과 관련된 표준 이벤트 (예: 구독 요청에 대한 승인) 를 Amazon에 DataZone 게시합니다. EventBridge 이러한 표준 이벤트를 사용하여 사용자 지정 통합을 위해 다른 AWS 서비스 또는 타사 솔루션과 통합할 수 있습니다.

주제

데이터 검색

다음 작업은 Amazon에서 데이터를 검색하는 다양한 방법을 설명합니다 DataZone.

주제

카탈로그에서 자산 검색 및 보기

DataZone Amazon은 데이터를 검색하는 간소화된 방법을 제공합니다. 데이터 포털에 액세스할 권한이 있는 모든 Amazon DataZone 사용자는 Amazon DataZone 카탈로그에서 자산을 검색하고 해당 자

산에 할당된 자산 이름 및 메타데이터를 볼 수 있습니다. 세부 정보 페이지를 검토하면 자산을 더 자세히 살펴볼 수 있습니다.

> **Note**
>
> 자산에 포함된 실제 데이터를 보려면 먼저 자산을 구독하고 구독 요청이 승인되고 액세스 권한이 부여되어야 합니다. 자세한 정보는 데이터 구독을 참조하세요.

카탈로그에서 자산을 검색하려면

1. Amazon DataZone 데이터 포털 URL로 이동하여 싱글 사인온 (SSO) 또는 자격 증명을 사용하여 로그인합니다. AWS Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 위치로 로그인한 다음 Open data portal을 선택할 수 있습니다.
2. 데이터 포털 홈 페이지의 검색 창에 찾으려는 자산의 이름을 입력할 수 있습니다.
3. 네임스페이스를 탐색하려면 페이지 오른쪽 상단에서 카탈로그를 선택하여 카탈로그를 엽니다. 카탈로그는 데이터 소유자 및 용어집 용어와 같은 기준으로 검색하여 자산을 찾을 수 있는 다양한 검색 환경을 제공합니다.
4. 검색 상자 중 하나에 검색어를 입력합니다. 검색을 실행한 후 다양한 필터를 적용하여 결과 범위를 좁힐 수 있습니다. 필터에는 자산 유형, 소스 계정 및 자산이 AWS 리전 속한 대상이 포함됩니다.
5. 특정 자산에 대한 세부 정보를 보려면 자산을 선택하여 해당 세부 정보 페이지를 엽니다. 세부정보 페이지에는 다음 정보가 포함됩니다.

   - 자산 이름, 데이터 소스 (AWS Glue Amazon Redshift 또는 Amazon S3), 유형 (테이블, 뷰 또는 S3 객체), 열 수, 크기
   - 자산에 대한 설명.
   - 자산의 현재 게시된 버전, 소유자, 구독에 대한 승인이 필요한지 여부, 네임스페이스, 업데이트 기록.
   - 용어집 용어 및 메타데이터 양식이 포함된 개요 탭
   - 비즈니스 및 기술 컬럼 이름, 데이터 유형, 컬럼의 비즈니스 설명 등 자산의 스키마를 표시하는 스키마 탭입니다. 스키마 탭은 테이블과 뷰에만 표시되며 Amazon S3 객체에는 표시되지 않습니다.
   - 도메인 구독자 목록이 포함된 구독 탭.
   - 자산의 과거 수정 목록이 포함된 기록 탭.

데이터 구독

다음 작업은 DataZone Amazon의 자산 구독에 대한 세부 정보를 제공합니다.

주제

자산 구독 요청

DataZone Amazon에서는 Amazon DataZone 카탈로그의 자산을 찾고, 액세스하고, 사용할 수 있습니다. 카탈로그에서 액세스하려는 자산을 찾으면 해당 자산을 구독해야 합니다. 그러면 구독 요청이 생성됩니다. 그러면 승인자가 요청을 승인하거나 요청할 수 있습니다.

프로젝트 내 자산에 대한 구독을 요청하려면 프로젝트의 멤버여야 합니다.

에셋을 구독하려면

1. Amazon DataZone 데이터 포털 URL로 이동하여 싱글 사인온 (SSO) 또는 자격 증명을 사용하여 로그인합니다. AWS Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 위치로 로그인한 다음 Open data portal을 선택할 수 있습니다.
2. 검색 창을 사용하여 구독하려는 자산을 검색하고 선택한 다음 구독을 선택합니다.
3. 구독 팝업 창에서 다음 정보를 제공하십시오.
   - 에셋에 구독하려는 프로젝트
   - 구독 요청에 대한 간략한 근거.
4. 구독을 선택합니다.

   게시자가 요청을 승인하면 데이터 포털에서 알림을 받게 됩니다.

구독 요청 상태를 보려면 자산에 가입한 프로젝트를 찾아 선택하십시오. 프로젝트의 데이터 탭으로 이동한 다음 왼쪽 탐색 창에서 요청된 데이터를 선택합니다. 이 페이지에는 프로젝트에서 액세스를 요청한 에셋이 나열됩니다. 요청 상태별로 목록을 필터링할 수 있습니다.

구독 요청 승인 또는 거부

DataZone Amazon에서는 Amazon DataZone 카탈로그의 자산을 찾고, 액세스하고, 사용할 수 있습니다. 카탈로그에서 액세스하려는 자산을 찾으면 해당 자산을 구독해야 합니다. 그러면 구독 요청이 생성됩니다. 그러면 승인자가 요청을 승인하거나 거부할 수 있습니다.

소유 프로젝트 (자산을 게시한 프로젝트) 의 멤버여야 구독 요청을 승인하거나 거부할 수 있습니다.

구독 요청을 승인 또는 거부하려면

1. Amazon DataZone 데이터 포털 URL로 이동하여 싱글 사인온 (SSO) 또는 자격 증명을 사용하여 로그인합니다. AWS Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 위치로 로그인한 다음 Open data portal을 선택할 수 있습니다.
2. 데이터 포털에서 프로젝트 목록 찾아보기를 선택하고 구독 요청과 함께 자산이 포함된 프로젝트를 선택합니다.
3. 데이터 탭으로 이동한 다음 왼쪽 탐색 창에서 수신 요청을 선택합니다.
4. 요청을 찾아 요청 보기를 선택합니다. 보류 중으로 필터링하여 아직 진행 중인 요청만 볼 수 있습니다.
5. 구독 요청과 액세스 사유를 검토하고 승인 또는 거부 여부를 결정하십시오.
6. (선택 사항) 요청을 수락하거나 거부한 이유를 설명하는 답변을 입력합니다.
7. 승인 또는 거부를 선택합니다.

프로젝트 소유자는 언제든지 구독을 취소할 수 있습니다. 자세한 정보는 the section called “기존 구독 취소”을 참조하세요.

모든 구독 요청을 보려면 을 참조하십시오. Amazon DataZone 이벤트 및 알림 사용하기

기존 구독 취소

DataZone Amazon에서는 Amazon DataZone 카탈로그의 자산을 찾고, 액세스하고, 사용할 수 있습니다. 카탈로그에서 액세스하려는 자산을 찾으면 해당 자산을 구독해야 합니다. 그러면 구독 요청이 생성됩니다. 그러면 승인자가 요청을 승인하거나 요청할 수 있습니다. 승인이 잘못되었거나 구독자가 더 이상 자산에 액세스할 필요가 없기 때문에 승인한 후 구독을 취소해야 할 수 있습니다.

구독을 취소하려면 소유 프로젝트 (자산을 게시한 프로젝트) 의 멤버여야 합니다.

구독을 취소하려면

1. Amazon DataZone 데이터 포털 URL로 이동하여 싱글 사인온 (SSO) 또는 자격 증명을 사용하여 로그인합니다. AWS Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 위치로 로그인한 다음 Open data portal을 선택할 수 있습니다.
2. 상단 탐색 창에서 프로젝트 선택을 선택하고 취소하려는 구독이 포함된 프로젝트를 선택합니다.
3. 데이터 탭으로 이동한 다음 왼쪽 탐색 창에서 수신 요청을 선택합니다.
4. 취소하려는 구독을 찾아 구독 보기를 선택합니다.
5. (선택 사항) 구독자가 자산을 프로젝트의 구독 대상에 유지할 수 있도록 하려면 확인란을 활성화합니다. 구독 대상은 환경 내에서 구독한 데이터를 사용할 수 있는 리소스 집합에 대한 참조입니다.

   나중에 구독 대상에서 자산에 대한 액세스 권한을 취소하려면 에서 취소해야 합니다. AWS Lake Formation
6. 구독 취소를 선택합니다.

구독을 취소한 후에는 구독을 다시 승인할 수 없습니다. 구독자가 자산을 다시 구독해야 승인할 수 있습니다.

구독 요청 취소

DataZone Amazon에서는 Amazon DataZone 카탈로그의 자산을 찾고, 액세스하고, 사용할 수 있습니다. 카탈로그에서 액세스하려는 자산을 찾으면 해당 자산을 구독해야 합니다. 그러면 구독 요청이 생성됩니다. 그러면 승인자가 요청을 승인하거나 요청할 수 있습니다. 보류 중인 구독 요청을 실수로 제출했거나 자산에 대한 읽기 권한이 더 이상 필요하지 않기 때문에 취소해야 할 수 있습니다.

구독 요청을 취소하려면 프로젝트 소유자 또는 기여자여야 합니다.

구독 요청을 취소하려면

1. Amazon DataZone 데이터 포털 URL로 이동하여 싱글 사인온 (SSO) 또는 자격 증명을 사용하여 로그인합니다. AWS Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 위치로 로그인한 다음 Open data portal을 선택할 수 있습니다.
2. 상단 탐색 창에서 프로젝트 선택을 선택하고 구독 요청이 포함된 프로젝트를 선택합니다.

3. 프로젝트의 데이터 탭으로 이동한 다음 왼쪽 탐색 창에서 요청된 데이터를 선택합니다. 이 페이지에는 프로젝트에서 액세스를 요청한 에셋이 나열됩니다.
4. 요청별로 필터링하면 아직 보류 중인 요청만 볼 수 있습니다. 요청을 찾아 요청 보기를 선택합니다.
5. 구독 요청을 검토하고 요청 취소를 선택합니다.

자산 (또는 다른 자산) 을 재구독하려면 을 참조하십시오the section called “자산 구독 요청”.

자산 구독 취소

DataZone Amazon에서는 Amazon DataZone 카탈로그의 자산을 찾고, 액세스하고, 사용할 수 있습니다. 카탈로그에서 액세스하려는 자산을 찾으면 해당 자산을 구독해야 합니다. 그러면 구독 요청이 생성됩니다. 그러면 승인자가 요청을 승인하거나 요청할 수 있습니다. 실수로 구독하여 승인을 받았거나 자산에 대한 읽기 권한이 더 이상 필요하지 않기 때문에 자산 구독을 취소해야 할 수 있습니다.

프로젝트의 에셋 중 하나를 구독 취소하려면 프로젝트의 멤버여야 합니다.

에셋 구독 취소하기

1. Amazon DataZone 데이터 포털 URL로 이동하여 싱글 사인온 (SSO) 또는 자격 증명을 사용하여 로그인합니다. AWS Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 위치로 로그인한 다음 Open data portal을 선택할 수 있습니다.
2. 상단 탐색 창에서 프로젝트 선택을 선택하고 구독을 취소하려는 자산이 포함된 프로젝트를 선택합니다.
3. 프로젝트의 데이터 탭으로 이동한 다음 왼쪽 탐색 창에서 요청된 데이터를 선택합니다. 이 페이지에는 프로젝트에서 액세스를 요청한 에셋이 나열됩니다.
4. 승인된 요청만 보려면 승인됨으로 필터링하십시오. 요청을 찾아 구독 보기를 선택합니다.
5. 구독을 검토하고 구독 취소를 선택합니다.

자산 (또는 다른 자산) 을 재구독하려면 을 참조하십시오. the section called “자산 구독 요청”

기존 IAM 역할을 사용하여 Amazon DataZone 구독 처리

현재 릴리스에서 DataZone Amazon은 기존 IAM 역할을 사용하여 데이터에 액세스할 수 있도록 지원합니다. 이를 위해 Amazon DataZone 환경에서 구독을 이행하는 데 사용하는 구독 대상을 생성할 수

있습니다. 연결된 AWS 계정 중 하나에 환경에 대한 구독 대상을 생성하려면 다음 단계를 사용할 수 있습니다.

1단계: Amazon DataZone 도메인이 버전 2 이상의 RAM 정책을 사용하고 있는지 확인

1. AWS RAM 콘솔의 Shared by me: 리소스 공유 페이지로 이동합니다.
2. AWS RAM 리소스 공유는 특정 AWS 지역에 존재하므로 콘솔 오른쪽 상단의 드롭다운 목록에서 적절한 AWS 지역을 선택합니다.
3. Amazon DataZone 도메인에 해당하는 리소스 공유를 선택한 다음 [Modify] 를 선택합니다. :라는 이름으로 RAM 공유가 생성되므로 DataZone 도메인의 이름 또는 ID를 사용하여 Amazon 도메인의 RAM 공유를 식별할 수 `DataZone-<domain-name>-<domain-id>` 있습니다.
4. 다음을 선택하여 RAM 정책의 버전을 확인하고 수정할 수 있는 다음 단계로 진행합니다.
5. RAM 정책 버전이 버전 2 이상인지 확인하십시오. 그렇지 않은 경우 드롭다운을 사용하여 버전 2 이상을 선택하십시오.
6. 4단계: 검토 및 업데이트로 건너뛰기를 선택합니다.
7. 리소스 공유 업데이트를 선택합니다.

2단계: 연결된 계정에서 구독 대상 만들기

- 현재 릴리스에서 Amazon은 API만을 사용하여 구독 대상을 생성할 수 있도록 DataZone 지원합니다. 다음은 AWS Glue 테이블 및 Amazon Redshift 테이블 또는 뷰에 대한 구독을 이행하기 위한 구독 대상을 생성하는 데 사용할 수 있는 페이로드의 몇 가지 예입니다. 자세한 내용은 을 참조하십시오. CreateSubscriptionTarget

  AWS Glue 구독 대상 예시

```
{
        "domainIdentifier": "<DOMAIN_ID>",
        "environmentIdentifier": "<ENVIRONMENT_ID>",
        "name": "<SUBSCRIPTION_TARGET_NAME>",
        "type": "GlueSubscriptionTargetType",
        "authorizedPrincipals" : ["IAM_ROLE_ARN"],
        "subscriptionTargetConfig" : [{"content": "{\"databaseName\":
 \"<DATABASE_NAME>\"}", "formName": "GlueSubscriptionTargetConfigForm"}],
        "manageAccessRole": "<GLUE_DATA_ACCESS_ROLE_IN_ASSOCIATED_ACCOUNT_ARN>",
        "applicableAssetTypes" : ["GlueTableAssetType"],
        "provider": "Amazon DataZone"
```

```
}
```

Amazon Redshift의 구독 대상 예시:

```
{
        "domainIdentifier": "<DOMAIN_ID>",
        "environmentIdentifier": "<ENVIRONMENT_ID>",
        "name": "<SUBSCRIPTION_TARGET_NAME>",
        "type": "RedshiftSubscriptionTargetType",
        "authorizedPrincipals" : ["REDSHIFT_DATABASE_ROLE_NAME"],
        "subscriptionTargetConfig" : [{"content": "{\"databaseName\":
 \"<DATABASE_NAME>\", \"secretManagerArn\": \"<SECRET_MANAGER_ARN>
\",\"clusterIdentifier\": \"<CLUSTER_IDENTIFIER>\"}", "formName":
 "RedshiftSubscriptionTargetConfigForm"}],
        "manageAccessRole":
 "<REDSHIFT_DATA_ACCESS_ROLE_IN_ASSOCIATED_ACCOUNT_ARN>",
        "applicableAssetTypes" : ["RedshiftViewAssetType",
 "RedshiftTableAssetType"],
        "provider": "Amazon DataZone"
}
```

Important

- 위의 API 호출에서 사용한 환경 식별자는 API 호출을 수행하는 데 사용한 것과 동일한 관련 계정에 있어야 합니다. 그렇지 않으면 API 호출이 성공하지 못합니다.
- “AuthorizedPrincipals”에서 사용하는 IAM 역할 ARN은 구독 자산이 구독 대상에 추가된 후 DataZone Amazon에서 액세스 권한을 부여하는 역할입니다. 이러한 승인된 보안 주체는 구독 대상이 생성되는 환경과 동일한 계정에 속해야 합니다.
- Amazon에서 구독 처리를 완료하려면 공급자 필드의 값이 DataZone “Amazon DataZone ”이어야 합니다.
- 에서 입력한 데이터베이스 이름은 대상이 생성되는 계정에 이미 subscriptionTargetConfig 존재해야 합니다. DataZone Amazon은 이 데이터베이스를 생성하지 않습니다. 또한 액세스 관리 역할에 이 데이터베이스에 대한 CREATE TABLE 권한이 있는지 확인하십시오.

- 또한 승인된 보안 주체로 제공되는 역할 (AWS Glue의 경우 IAM 역할 및 Amazon Redshift의 데이터베이스 역할) 이 환경 계정에 이미 존재하는지 확인하십시오. Amazon Redshift 구독 대상의 경우 클러스터에 연결하는 동안 역할을 맡으려면 추가 업데이트가 필요합니다. 이 역할에는 역할에 RedshiftDbRoles 태그가 첨부되어 있어야 합니다. 태그의 값은 쉼표로 구분된 목록일 수 있습니다. 값은 구독 대상을 만들 때 승인된 주체로 제공된 데이터베이스 역할이어야 합니다.

3단계: 새 테이블 구독 및 새 대상에 대한 구독 이행

- 구독 대상을 생성한 후에는 새 테이블을 구독할 수 있으며 DataZone Amazon은 위 목표에 맞춰 해당 테이블을 처리합니다. 자세한 정보는 데이터 구독을 참조하세요.

데이터 액세스 권한 부여

다음 작업은 Amazon 자산에 승인된 구독에 대한 액세스 권한을 부여하는 방법에 대한 세부 정보를 제공합니다. DataZone

DataZoneAmazon에서는 구독 승인자가 구독 요청과 자산에 대한 읽기 액세스 권한을 승인하거나 부여한 구독을 관리합니다. 자산에 대한 구독 승인자는 해당 자산이 Amazon DataZone 카탈로그에 게시된 게시 계약에 따라 결정됩니다.

주제

- 관리 AWS Glue Data Catalog 자산에 대한 액세스 권한 부여
- 관리형 Amazon Redshift 자산에 대한 액세스 권한 부여
- 비관리 자산에 대한 승인된 구독에 대한 액세스 권한을 부여하십시오.

관리 AWS Glue Data Catalog 자산에 대한 액세스 권한 부여

> **Note**
>
> AWS Lake Formation LF-TBAC 방법을 사용한 AWS Glue Data Catalog 자산에 대한 액세스 관리는 지원되지 않습니다.
> 의 에셋에 AWS Glue Data Catalog 대한 지역 간 공유 지원은 지원되지 않습니다.

관리 AWS Glue Data Catalog 자산에 대한 구독 요청이 승인되면 Amazon은 이러한 자산을 프로젝트의 모든 기존 데이터 레이크 환경에 DataZone 자동으로 추가합니다. DataZone 그러면 Amazon이 사용자를 대신하여 승인된 AWS Glue Data Catalog 테이블에 대한 액세스 권한을 부여하고 관리합니다 AWS Lake Formation. 구독자 프로젝트의 경우 부여된 자산은 계정의 AWS Glue Data Catalog as 리소스에 표시됩니다. 그런 다음 Amazon Athena를 사용하여 테이블을 쿼리할 수 있습니다.

> **Note**
>
> 구독한 AWS Glue Data Catalog 자산이 기존 데이터 레이크 환경에 자동으로 추가된 후 새 데이터 레이크 환경을 프로젝트에 추가하는 경우, 구독한 AWS Glue Data Catalog 자산을 이 새 데이터 레이크 환경에 수동으로 추가해야 합니다. Amazon DataZone 데이터 포털의 프로젝트 개요 페이지에 있는 데이터 탭에서 보조금 추가 옵션을 선택하면 됩니다.

DataZone Amazon이 AWS Glue Data Catalog 테이블에 대한 액세스 권한을 부여할 수 있으려면 다음 조건을 충족해야 합니다.

- Amazon은 Lake Formation 권한을 관리하여 액세스 권한을 DataZone 부여하므로 AWS Glue 테이블은 Lake Formation에서 관리해야 합니다.
- AWS Glue Data Catalog 테이블을 게시하는 데 사용되는 데이터 레이크 환경의 관리 액세스 역할에는 다음과 같은 Lake Formation 권한이 있어야 합니다.
  - `DESCRIBE`및 게시된 테이블이 포함된 AWS Glue 데이터베이스에 대한 `DESCRIBE GRANTABLE` 권한
  - `DESCRIBE`,`SELECT`,`DESCRIBE GRANTABLE`, 게시된 테이블 자체에 대한 Lake Formation의 `SELECT GRANTABLE` 권한

자세한 내용은 개발자 안내서의 카탈로그 리소스에 대한 권한 부여 및 취소를 참조하십시오.AWS Lake Formation

관리형 Amazon Redshift 자산에 대한 액세스 권한 부여

Amazon Redshift 테이블 또는 뷰에 대한 구독이 승인되면 DataZone Amazon은 구독한 자산을 프로젝트 내의 모든 데이터 웨어하우스 환경에 자동으로 추가하여 프로젝트 구성원이 환경 내에서 Amazon Redshift 쿼리 편집기 링크를 사용하여 데이터를 쿼리할 수 있습니다. DataZoneAmazon은 내부적으로 소스와 구독 대상 간에 필요한 권한 부여 및 데이터 공유를 생성합니다.

액세스 권한 부여 프로세스는 원본 데이터베이스 (게시자) 와 대상 데이터베이스 (구독자) 의 위치에 따라 다릅니다.

- 동일한 클러스터, 동일한 데이터베이스 - 동일한 데이터베이스 내에서 데이터를 공유해야 하는 경우 Amazon은 원본 테이블에 대한 권한을 직접 DataZone 부여합니다.
- 동일한 클러스터, 다른 데이터베이스 - 동일한 클러스터 내의 두 데이터베이스에서 데이터를 공유해야 하는 경우 Amazon은 대상 데이터베이스에 뷰를 DataZone 생성하고 생성된 뷰에 대한 권한을 부여합니다.
- 동일 계정 다른 클러스터 - DataZone Amazon은 소스 클러스터와 대상 클러스터 간에 데이터 공유를 생성하고 공유 테이블 위에 뷰를 생성합니다. 뷰에 권한이 부여됩니다.
- 교차 계정 - 위와 동일하지만 생산자 클러스터 측에서 계정 간 데이터 공유를 승인하려면 추가 단계가 필요하고 소비자 클러스터 측에서 데이터 공유를 연결하려면 다른 단계가 필요합니다.

> **Note**
>
> 구독한 Amazon Redshift 자산이 기존 데이터 웨어하우스 환경에 자동으로 추가된 후 새 데이터 웨어하우스 환경을 프로젝트에 추가하는 경우, 구독한 Amazon Redshift 자산을 이 새 데이터 웨어하우스 환경에 수동으로 추가해야 합니다. Amazon DataZone 데이터 포털의 프로젝트 개요 페이지에 있는 데이터 탭에서 보조금 추가 옵션을 선택하면 됩니다.

Amazon Redshift 게시 및 구독 클러스터가 Amazon Redshift 데이터 공유에 대한 모든 요구 사항을 충족하는지 확인하십시오. 자세한 내용은 Amazon Redshift 개발자 안내서를 참조하십시오.

> **Note**
>
> DataZone Amazon은 Amazon Redshift 클러스터와 Amazon Redshift 서버리스 자산 모두에 대한 구독을 자동으로 허용하는 기능을 지원합니다.
> Amazon Redshift를 사용한 지역 간 데이터 공유는 지원되지 않습니다.

> **Note**
>
> 현재 릴리스에서 Amazon은 소스 및 대상 Amazon Redshift 클러스터 또는 작업 그룹이 동일한 조직에 속한 계정에 있는 경우에만 Amazon Redshift 테이블 및 뷰에 AWS 대한 액세스를 관리할 DataZone 수 있습니다. AWS

비관리 자산에 대한 승인된 구독에 대한 액세스 권한을 부여하십시오.

Amazon에서는 DataZone 사용자가 비즈니스 데이터 카탈로그에 모든 유형의 자산을 게시할 수 있습니다. 이러한 자산 중 일부에 대해 Amazon은 액세스 허가를 자동으로 관리할 DataZone 수 있습니다. 이러한 자산을 관리 자산이라고 하며, 여기에는 Lake Formation에서 관리하는 AWS Glue 데이터 카탈로그 테이블과 Amazon Redshift 테이블 및 뷰가 포함됩니다. Amazon에서 구독을 자동으로 DataZone 승인할 수 없는 다른 모든 자산을 비관리형 자산이라고 합니다.

DataZone Amazon은 관리되지 않는 자산에 대한 액세스 권한을 관리할 수 있는 경로를 제공합니다. 데이터 소유자가 비즈니스 데이터 카탈로그의 자산에 대한 구독을 승인하면 Amazon은 소스와 대상 간에 액세스 권한을 생성할 수 있도록 페이로드의 모든 필수 정보와 함께 EventBridge Amazon에 이벤트를 DataZone 게시합니다. 이 이벤트를 수신하면 이벤트의 정보를 사용하여 필요한 부여 또는 권한을 생성할 수 있는 사용자 지정 핸들러를 트리거할 수 있습니다. 액세스 권한을 부여한 후에는 Amazon에서 구독 상태를 보고하고 DataZone 업데이트하여 자산을 구독한 사용자에게 자산 사용을 시작할 수 있음을 알릴 수 있습니다. 자세한 정보는 Amazon DataZone 이벤트 및 알림 사용하기을 참조하세요.

소비 데이터

다음 작업은 DataZone Amazon에서 구독한 소비 데이터에 대한 세부 정보를 제공합니다.

주제

- 아마존 아테나 또는 아마존 Redshift에서 데이터 쿼리

아마존 아테나 또는 아마존 Redshift에서 데이터 쿼리

Amazon에서는 구독자가 카탈로그의 자산에 액세스하면 Amazon DataZone Athena 또는 Amazon Redshift 쿼리 편집기 v2를 사용하여 해당 자산을 사용 (쿼리 및 분석) 할 수 있습니다. 이 작업을 완료하려면 프로젝트 소유자 또는 기여자여야 합니다. 프로젝트에서 활성화된 블루프린트에 따라 Amazon은 데이터 포털의 프로젝트 페이지 오른쪽 창에 Amazon Athena 및/또는 Amazon Redshift 쿼리 편집기 v2로 연결되는 링크를 DataZone 제공합니다.

1. Amazon DataZone 데이터 포털 URL로 이동하여 싱글 사인온 (SSO) 또는 자격 증명을 사용하여 로그인합니다. AWS Amazon DataZone 관리자인 경우 https://console.aws.amazon.com/datazone 에서 Amazon DataZone 콘솔로 이동하여 도메인이 생성된 AWS 계정 위치로 로그인한 다음 Open data portal을 선택할 수 있습니다.
2. Amazon DataZone 데이터 포털에서 프로젝트 목록 찾아보기를 선택한 다음 분석하려는 데이터가 있는 프로젝트를 찾아 선택합니다.

3. 이 프로젝트에서 Data Lake 블루프린트가 활성화된 경우 Amazon Athena로 연결되는 링크가 프로젝트 홈 페이지의 오른쪽 패널에 표시됩니다.

   이 프로젝트에서 데이터 웨어하우스 블루프린트가 활성화된 경우 프로젝트 홈 페이지의 오른쪽 패널에 쿼리 편집기로 연결되는 링크가 표시됩니다.

> **Note**
>
> 블루프린트는 프로젝트가 생성되는 환경 프로파일에 정의됩니다.

주제

- Amazon Athena를 사용하여 데이터를 쿼리합니다.
- Amazon Redshift를 사용하여 데이터를 쿼리합니다.

Amazon Athena를 사용하여 데이터를 쿼리합니다.

Amazon Athena 링크를 선택하면 인증용 프로젝트 자격 증명을 사용하여 브라우저의 새 탭에서 Amazon Athena 쿼리 편집기가 열립니다. 작업 중인 Amazon DataZone 프로젝트가 쿼리 편집기에서 현재 작업 그룹으로 자동 선택됩니다.

Amazon Athena 쿼리 편집기에서 쿼리를 작성하고 실행합니다. 몇 가지 일반적인 작업은 다음과 같습니다.

- 구독한 자산을 쿼리하고 분석하세요.
- 새 테이블 생성
- 외부 S3 버킷의 쿼리 결과 (CTAS) 에서 테이블을 생성합니다.

구독한 자산을 쿼리하고 분석하세요.

프로젝트가 구독한 자산에 대한 액세스 권한을 DataZone Amazon에서 자동으로 부여하지 않는 경우 기본 데이터에 대한 액세스 권한을 부여해야 합니다. 이러한 자산에 대한 액세스 권한을 부여하는 방법에 대한 자세한 내용은 을 참조하십시오비관리 자산에 대한 승인된 구독에 대한 액세스 권한을 부여하십시오..

Amazon에서 프로젝트가 구독한 자산에 대한 액세스 권한을 자동으로 부여하는 경우 DataZone, 테이블에서 SQL 쿼리를 실행하고 Amazon Athena에서 결과를 확인할 수 있습니다. Amazon Athena에서 SQL을 사용하는 방법에 대한 자세한 내용은 Athena에 대한 SQL 참조를 참조하십시오.

프로젝트 홈 페이지의 오른쪽 패널에서 Amazon Athena 링크를 선택한 후 Amazon Athena 쿼리 편집기로 이동하면 Amazon Athena 쿼리 편집기의 오른쪽 상단에 프로젝트 드롭다운이 표시되고 프로젝트 컨텍스트가 자동으로 선택됩니다.

데이터베이스 드롭다운에서 다음 데이터베이스를 볼 수 있습니다.

- 퍼블리싱 데이터베이스 (*{environmentname}*_pub_db). 이 데이터베이스의 목적은 프로젝트 컨텍스트 내에서 새 데이터를 생성한 다음 이 데이터를 Amazon DataZone 카탈로그에 게시할 수 있는 환경을 제공하는 것입니다. 프로젝트 소유자와 기여자는 이 데이터베이스에 대한 읽기 및 쓰기 액세스 권한을 가집니다. 프로젝트 뷰어는 이 데이터베이스에 대한 읽기 권한만 가집니다.
- 구독 데이터베이스 (*{environmentname}*_sub_db). 이 데이터베이스의 목적은 Amazon DataZone 카탈로그에서 프로젝트 멤버로 구독한 데이터를 공유하고 해당 데이터를 쿼리할 수 있도록 하는 것입니다.

새 테이블 생성

외부 S3 버킷에 연결한 경우 Amazon Athena를 사용하여 외부 Amazon S3 버킷에서 자산을 쿼리하고 분석할 수 있습니다. 이 시나리오에서 DataZone Amazon은 외부 Amazon S3 버킷의 기본 데이터에 직접 액세스 권한을 부여할 권한이 없으며, 프로젝트 외부에서 생성된 외부 Amazon S3 데이터는 Lake Formation에서 자동으로 관리되지 않으므로 Amazon에서 관리할 수 없습니다 DataZone. 다른 방법은 Amazon Athena의 `CREATE TABLE` 명령문을 사용하여 외부 Amazon S3 버킷의 데이터를 프로젝트의 Amazon S3 버킷 내 새 테이블로 복사하는 것입니다. Amazon Athena에서 `CREATE TABLE` 쿼리를 실행하면 테이블을 에 등록합니다. AWS Glue Data Catalog

Amazon S3의 데이터에 대한 경로를 지정하려면 다음 예와 같이 `LOCATION` 속성을 사용합니다.

```
CREATE EXTERNAL TABLE 'test_table'(
...
)
ROW FORMAT ...
STORED AS INPUTFORMAT ...
OUTPUTFORMAT ...
LOCATION 's3://bucketname/folder/'
```

자세한 내용은 Amazon S3의 테이블 위치를 참조하십시오.

외부 S3 버킷의 쿼리 결과 (CTAS) 에서 테이블을 생성합니다.

자산을 구독하면 기본 데이터에 대한 액세스는 읽기 전용입니다. Amazon Athena를 사용하여 테이블 사본을 생성할 수 있습니다. Amazon Athena에서 A CREATE TABLE AS SELECT (CTAS) 쿼리는 다른 쿼리의 SELECT 명령문 결과를 바탕으로 Amazon Athena에 새 테이블을 생성합니다. CTAS 구문에 대한 자세한 내용은 테이블 AS 생성을 참조하십시오.

다음 예제에서는 테이블의 모든 열을 복사해 테이블을 만듭니다.

```
CREATE TABLE new_table AS
SELECT *
FROM old_table;
```

동일한 예제의 다음 변형에서 SELECT 문에는 WHERE 절이 포함되어 있습니다. 이 경우, 쿼리는 테이블에서 WHERE 절을 충족하는 행만 선택합니다.

```
CREATE TABLE new_table AS
SELECT *
FROM old_table WHERE condition;
```

다음 예제에서는 다른 테이블의 열 세트에 대해 실행할 새 쿼리를 생성합니다.

```
CREATE TABLE new_table AS
SELECT column_1, column_2, ... column_n
FROM old_table;
```

동일한 예제의 이번 변형에서는 여러 테이블의 특정 열을 바탕으로 새 테이블을 생성합니다.

```
CREATE TABLE new_table AS
SELECT column_1, column_2, ... column_n
FROM old_table_1, old_table_2, ... old_table_n;
```

새로 생성된 테이블은 이제 프로젝트 AWS Glue 데이터베이스의 일부가 되며, 데이터를 Amazon 카탈로그에 자산으로 게시하여 다른 사람이 검색하고 다른 Amazon DataZone 프로젝트와 공유할 수 있습니다. DataZone

Amazon Redshift를 사용하여 데이터를 쿼리합니다.

Amazon DataZone 데이터 포털에서 데이터 웨어하우스 청사진을 사용하는 환경을 엽니다. 환경 페이지의 오른쪽 패널에서 Amazon Redshift 링크를 선택합니다. 그러면 Amazon Redshift 쿼리 편집기 v2.0에서 환경의 Amazon Redshift 클러스터 또는 Amazon Redshift 서버리스 워크그룹에 연결하는 데 도움이 되는 필수 세부 정보가 포함된 확인 대화 상자가 열립니다. 연결을 설정하는 데 필요한 세부 정보를 확인했으면 Amazon Redshift 열기 버튼을 선택합니다. 그러면 Amazon 환경의 임시 자격 증명을 사용하여 브라우저의 새 탭에서 Amazon Redshift 쿼리 편집기 v2.0이 열립니다. DataZone

쿼리 편집기에서 사용 중인 환경이 Amazon Redshift 서버리스 워크그룹을 사용하는지 아니면 Amazon Redshift 클러스터를 사용하는지에 따라 아래 단계를 따르십시오.

Amazon Redshift 서버리스 워크그룹의 경우

1. 쿼리 편집기에서 Amazon DataZone 환경의 Amazon Redshift 서버리스 워크그룹을 식별하고 마우스 오른쪽 버튼으로 클릭한 다음 연결 생성을 선택합니다.
2. 인증을 위해 페더레이션 사용자를 선택합니다.
3. Amazon DataZone 환경 데이터베이스의 이름을 입력합니다.
4. 연결 생성을 선택합니다.

Amazon Redshift 클러스터의 경우:

1. 쿼리 편집기에서 Amazon DataZone 환경의 Amazon Redshift 클러스터를 식별하고 마우스 오른쪽 버튼으로 클릭한 다음 연결 생성을 선택합니다.
2. 인증을 위해 IAM ID를 사용하는 임시 자격 증명을 선택합니다.
3. 위의 인증 방법을 사용할 수 없는 경우 왼쪽 하단의 기어 버튼을 선택하여 계정 설정을 열고 IAM 자격 증명으로 인증을 선택한 다음 저장하십시오. 이 설정은 다음과 같습니다. one-time-only
4. 연결을 생성할 Amazon DataZone 환경 데이터베이스의 이름을 입력합니다.
5. 연결 생성을 선택합니다.

이제 Amazon 환경에 맞게 구성된 Amazon Redshift 클러스터 또는 Amazon Redshift 서버리스 워크그룹 내의 테이블과 뷰에 대해 쿼리를 시작할 수 있습니다. DataZone

구독한 모든 Amazon Redshift 테이블 또는 뷰는 해당 환경에 맞게 구성된 Amazon Redshift 클러스터 또는 Amazon Redshift 서버리스 작업 그룹에 연결됩니다. 테이블과 뷰를 구독할 수 있을 뿐만 아니라 환경의 클러스터 또는 데이터베이스에서 생성한 새 테이블과 뷰를 게시할 수 있습니다.

예를 들어, 환경이 Amazon Redshift 클러스터와 해당 클러스터에서 호출된 데이터베이스에 연결되는 시나리오를 `redshift-cluster-1` 가정해 보겠습니다. `dev` Amazon DataZone 데이터 포털을 사용하면 환경에 추가된 테이블과 뷰를 쿼리할 수 있습니다. 데이터 포털의 오른쪽 창에 있는 `Analytics tools` 섹션에서 이 환경을 위한 Amazon Redshift 링크를 선택하면 쿼리 편집기가 열립니다. 그런 다음 `redshift-cluster-1` 클러스터를 마우스 오른쪽 버튼으로 클릭하고 IAM ID를 사용하는 임시 자격 증명을 사용하여 연결을 생성할 수 있습니다. 연결이 설정되면 개발 데이터베이스에서 해당 환경이 액세스할 수 있는 모든 테이블과 뷰를 볼 수 있습니다.

Amazon DataZone 이벤트 및 알림 사용하기

DataZone Amazon은 구독 요청, 업데이트, 의견 및 시스템 이벤트와 같은 데이터 포털 내의 중요한 활동을 지속적으로 알려줍니다. Amazon은 데이터 포털의 전용 수신함이나 Amazon EventBridge 기본 버스를 통해 메시지를 전송하여 이 정보를 DataZone 제공합니다.

주제

Amazon DataZone 데이터 포털의 전용 수신함을 통한 이벤트 처리

DataZone Amazon은 데이터 포털에 메시지를 보고 조치를 취할 수 있는 전용 수신함을 제공합니다. 최근 메시지는 홈페이지, 프로젝트 페이지, 카탈로그 페이지에도 표시됩니다. 예를 들어 사용자가 데이터 자산에 대한 액세스를 요청하면 해당 자산의 게시 프로젝트 소유자 및 기여자는 데이터 포털에서 요청을 확인하고, 조치가 취해지면 이 요청과 관련된 구독 프로젝트의 프로젝트 구성원은 데이터 포털의 알림을 볼 수 있습니다. 메시지에는 두 가지 유형이 있습니다.

- 태스크 - 이 메시지는 수신자에게 어딘가에 필요한 조치가 있음을 알립니다. 추적에 사용할 수 있는 선택적 상태 필드가 있습니다.
- 이벤트 - 이러한 메시지는 정보 제공용이며 상태가 지정되지 않습니다. 이벤트는 최근 업데이트에 대한 감사 추적을 제공합니다.

DataZoneAmazon에서는 다음 이벤트 유형에 대해 메시지가 생성됩니다.

이벤트 범주	이벤트 이름	이벤트 설명	이벤트 유형
구독	구독 요청이 생성되었습니다.	구독 요청이 생성되면 이벤트가 생성됩니다.	작업
구독	구독 요청이 수락되었습니다.	구독 요청이 수락되면 이벤트가 생성됩니다.	Event
구독	구독 요청이 거부되었습니다.	구독 요청이 거부되면 이벤트가 생성됩니다.	Event

이벤트 범주	이벤트 이름	이벤트 설명	이벤트 유형
구독	구독 요청이 삭제되었습니다.	구독 요청이 삭제되면 이벤트가 생성됩니다.	Event
프로젝트	프로젝트 생성 성공	프로젝트 생성이 성공하면 이벤트가 생성됩니다.	Event
프로젝트 멤버십	프로젝트 멤버 추가 성공	프로젝트에 새 멤버가 추가되면 이벤트가 생성됩니다.	Event
프로젝트 멤버십	프로젝트 멤버 제거 성공	멤버가 프로젝트에서 제거되면 이벤트가 생성됩니다.	Event
프로젝트 멤버십	프로젝트 멤버 역할 변경 성공	이벤트가 생성되었습니다. 프로젝트에서 구성원의 역할이 변경됩니다.	Event
환경	환경 배포가 시작되었습니다.	환경 배포가 시작될 때 이벤트가 생성됩니다.	Event
환경	환경 배포가 완료되었습니다.	환경 배포가 성공적으로 완료되면 이벤트가 생성됩니다.	Event
환경	환경 배포에 실패했습니다.	환경 배포가 실패하면 이벤트가 생성됩니다.	Event
환경	환경 배포 사용자 지정 워크플로가 시작됨	사용자 지정 워크플로가 있는 환경이 시작되면 이벤트가 생성됩니다.	Event

이벤트 범주	이벤트 이름	이벤트 설명	이벤트 유형
데이터 자산	인벤토리에 추가된 자산	새 데이터 자산이 인벤토리에 추가될 때 (즉, 카탈로그에 초안 상태로 추가될 때) 이벤트가 생성됩니다.	Event
데이터 자산	자산 공개	새 데이터 자산이 게시될 때 (예: 구독이 가능한 경우) 이벤트가 생성됩니다.	Event
데이터 자산	에셋 스키마가 변경되었습니다.	이전 수집 작업 이후 자산 스키마가 변경되면 이벤트가 생성됩니다.	Event
구독	구독이 생성되었습니다.	누군가가 데이터 자산 구독을 요청하면 이벤트가 생성됩니다.	작업
구독	구독이 승인되었습니다.	게시 프로젝트 소유자 또는 기여자가 구독을 승인하면 이벤트가 생성됩니다.	Event
구독	구독이 거부되었습니다.	게시 프로젝트 소유자 또는 기여자가 구독을 거부하면 이벤트가 생성됩니다.	Event
구독	구독이 삭제되었습니다.	구독자가 구독을 취소하면 이벤트가 생성됩니다.	Event

이벤트 범주	이벤트 이름	이벤트 설명	이벤트 유형
구독	구독 허가가 요청되었습니다.	누군가가 자산에 대한 액세스를 요청하면 이벤트가 생성됩니다.	Event
구독	구독 허가가 완료되었습니다.	게시 프로젝트 소유자 또는 기여자가 구독에 에셋 액세스 권한을 부여하면 이벤트가 생성됩니다.	Event
구독	구독 허가가 실패했습니다.	구독 허가가 실패하면 이벤트가 생성됩니다.	Event
구독	구독 허가 취소가 요청되었습니다.	게시 프로젝트 소유자 또는 기여자가 취소된 구독 허가를 시작하면 이벤트가 생성됩니다.	Event
구독	구독 허가 취소 완료	구독 허가 취소가 완료되면 이벤트가 생성됩니다.	Event
구독	구독 허가 취소에 실패했습니다.	구독 허가 취소가 실패하면 이벤트가 생성됩니다.	Event
자동 비즈니스 이름 생성	비즈니스 이름 생성 성공	자동화된 비즈니스 이름 생성 작업이 성공적으로 완료될 때 이벤트가 생성됩니다.	Event
자동 비즈니스 이름 생성	비즈니스 이름 생성 실패	자동 비즈니스 이름 생성 작업이 실패하면 이벤트가 생성됩니다.	Event

이벤트 범주	이벤트 이름	이벤트 설명	이벤트 유형
데이터 소스 실행	데이터 소스가 생성되었습니다.	새 데이터 소스가 생성되면 이벤트가 생성됩니다.	Event
데이터 소스 실행	데이터 소스 업데이트	기존 데이터 소스가 업데이트되면 이벤트가 생성됩니다.	Event
데이터 소스 실행	데이터 소스 실행이 트리거됨	데이터 소스 실행이 시작될 때 이벤트가 생성됩니다.	Event
데이터 소스 실행	데이터 소스 실행 성공	데이터 소스 실행이 성공하면 이벤트가 생성됩니다.	Event
데이터 소스 실행	데이터 소스 실행 실패	데이터 소스 실행이 실패하면 이벤트가 생성됩니다.	Event

데이터 포털 수신함에서 작업을 보려면 다음 단계를 완료하세요.

1. 데이터 포털 URL을 사용하여 Amazon DataZone 데이터 포털로 이동하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 도메인이 생성된 AWS 계정의 Amazon DataZone 콘솔에서 https://console.aws.amazon.com/datazone 에 액세스하여 데이터 포털 URL을 확인할 수 있습니다.
2. 데이터 포털에서 최근 작업 세트가 포함된 팝업을 보려면 검색 창 옆에 있는 종 모양 아이콘을 선택합니다.
3. 모든 작업을 보려면 모두 보기를 선택합니다. 이벤트 탭을 선택하여 보기를 변경하고 모든 이벤트를 볼 수 있습니다.
4. 이벤트 제목, 활성 또는 비활성 상태 또는 날짜 범위를 기준으로 검색을 필터링할 수 있습니다.
5. 개별 작업을 선택하여 작업에 응답할 수 있는 위치로 이동합니다.

데이터 포털 수신함에서 이벤트를 보려면 다음 단계를 완료하세요.

1. 데이터 포털 URL을 사용하여 Amazon DataZone 데이터 포털로 이동하고 SSO 또는 AWS 자격 증명을 사용하여 로그인합니다. Amazon DataZone 관리자인 경우 Amazon DataZone 루트 도메인이 생성된 AWS 계정의 Amazon DataZone 콘솔에서 https://console.aws.amazon.com/datazone 에 액세스하여 데이터 포털 URL을 확인할 수 있습니다.
2. 데이터 포털에서 최근 이벤트 세트의 팝업을 보려면 검색 창 옆에 있는 종 아이콘을 선택합니다.
3. 모든 이벤트를 보려면 모두 보기를 선택합니다. 태스크 탭을 선택하여 보기를 변경하고 모든 작업을 볼 수 있습니다.
4. 이벤트 제목 또는 날짜 범위를 기준으로 검색을 필터링합니다.
5. 개별 이벤트를 선택하여 해당 이벤트에 대한 세부 정보를 볼 수 있는 위치로 이동합니다.

Amazon EventBridge 기본 버스를 통한 이벤트 처리

데이터 포털의 전용 수신함으로 메시지를 보내는 것 외에도 Amazon DataZone 루트 도메인이 호스팅되는 동일한 AWS 계정의 Amazon EventBridge 기본 이벤트 버스로 이러한 메시지를 전송합니다. DataZone 이를 통해 구독 이행 또는 다른 도구와의 사용자 지정 통합과 같은 이벤트 기반 자동화가 가능합니다. 들어오는 Amazon EventBridge 이벤트와 일치하는 규칙을 생성하고 이를 Amazon EventBridge 대상으로 전송하여 처리할 수 있습니다. 단일 규칙으로 이벤트를 여러 대상으로 전송한 다음, 병렬로 실행할 수 있습니다.

샘플 이벤트는 다음과 같습니다.

```
{
  "version": "0",
  "id": "bd3d6239-2877-f464-0572-b1d76760e085",
  "detail-type": "Subscription Request Created",
  "source": "aws.datazone",
  "account": "111111111111",
  "time": "2023-11-13T17:57:00Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "version": "655",
    "metadata": {
      "domain": "dzd_bc8e1ez8r2a6xz",
      "user": "44f864b8-50a1-70cc-736f-c1f763934ab7",
      "id": "5jbc0lie0sr99j",
      "version": "1",
      "typeName": "SubscriptionRequestEntityType",
```

```
      "owningProjectId": "6oy92hwk937pgn",
      "awsAccountId": "111111111111",
      "clientToken": "e781b7b5-78c5-4608-961e-3792a6c3ff0d"
    },
    "data": {
      "autoApproved": true,
      "requesterId": "44f864b8-50a1-70cc-736f-c1f763934ab7",
      "status": "PENDING",
      "subscribedListings": [
        {
          "id": "ayzstznnx4dxyf",
          "ownerProjectId": "5a3se66qm88947",
          "version": "12"
        }
      ],
      "subscribedPrincipals": [
        {
          "id": "6oy92hwk937pgn",
          "type": "PROJECT"
        }
      ]
    }
  }
}
```

DataZone Amazon에서 지원하는 상세 유형의 전체 목록은 다음과 같습니다.

- 구독 요청 생성됨
- 구독 요청 수락됨
- 구독 요청 거부됨
- 구독 요청 삭제됨
- 구독 허가가 요청되었습니다.
- 구독 보조금 완료
- 구독 보조금 실패
- 구독 보조금 취소 요청
- 구독 보조금 취소 완료
- 구독 보조금 취소 실패
- 자산이 인벤토리에 추가됨

- 카탈로그에 추가된 자산
- 에셋 스키마 변경
- 데이터 소스 상태 변경
- 데이터 소스 생성됨
- 데이터 소스 업데이트
- 데이터 소스 실행이 트리거됨
- 데이터 소스 실행 성공
- 데이터 소스 실행 실패
- 도메인 생성 성공
- 도메인 생성 실패
- 도메인 삭제 성공
- 도메인 삭제 실패
- 환경 배포 시작됨
- 환경 배포 완료
- 환경 배포 실패
- 환경 삭제가 시작됨
- 환경 삭제가 완료되었습니다.
- 환경 삭제 실패
- 프로젝트 생성 성공
- 프로젝트 멤버 추가 성공
- 프로젝트 멤버 제거 성공
- 프로젝트 멤버 역할 변경 성공
- 환경 배포, 고객 워크플로가 시작되었습니다.
- 비즈니스 이름 생성 성공
- 비즈니스 이름 생성 실패

자세한 내용은 Amazon을 참조하십시오 EventBridge.

아마존의 보안 DataZone

클라우드 AWS 보안이 최우선 과제입니다. AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

보안은 기업과 귀사 간의 공동 책임입니다. AWS 공동 책임 모델은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호하는 역할을 합니다 AWS 클라우드. AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. DataZoneAmazon에 적용되는 규정 준수 프로그램에 대해 자세히 알아보려면 규정 준수 프로그램별 범위 내 서비스 규정 준수 참조하십시오.
- 클라우드에서의 보안 — 귀하의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터의 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 Amazon을 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 DataZone 됩니다. 다음 주제는 보안 및 규정 준수 목표를 DataZone 충족하도록 Amazon을 구성하는 방법을 보여줍니다. 또한 Amazon DataZone 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 알아봅니다.

주제

아마존에서의 데이터 보호 DataZone

AWS 공동 책임 모델 Amazon의 데이터 보호에 적용됩니다 DataZone. 이 모델에 설명된 대로 AWS 은(는) 모두를 실행하는 글로벌 인프라를 보호할 책임이 AWS 클라우드있습니다. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스 의 보안 구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은AWS 보안 블로그에서 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

데이터 보호를 위해 AWS 계정 자격 증명을 보호하고 AWS IAM Identity Center OR AWS Identity and Access Management (IAM) 을 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 멀티 팩터 인증 설정(MFA)을 사용하세요.
- SSL/TLS를 사용하여 리소스와 통신할 수 있습니다. AWS TLS 1.2는 필수이며 TLS 1.3를 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다. AWS CloudTrail
- 포함된 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용하십시오 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 API를 AWS 통해 액세스할 때 FIPS 140-2로 검증된 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용하십시오. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 FIPS(Federal Information Processing Standard) 140-2를 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 필드에 입력하지 않는 것이 좋습니다. 여기에는 Amazon DataZone 또는 다른 곳에서 콘솔 AWS CLI, API 또는 AWS SDK를 AWS 서비스 사용하여 작업하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 자격 보안 인증를 URL에 포함시켜서는 안 됩니다.

데이터 암호화

권한을 부여할 때는 누가 어떤 Amazon DataZone 리소스에 어떤 권한을 부여할지 결정합니다. 해당 리소스에서 허용할 작업을 사용 설정합니다. 따라서 작업을 수행하는 데 필요한 권한만 부여해야 합니다.

최소 권한 액세스를 구현하는 것이 오류 또는 악의적인 의도로 인해 발생할 수 있는 보안 위험과 영향을 최소화할 수 있는 근본적인 방법입니다.

저장 중 암호화

Amazon은 기본적으로 사용자를 대신하여 AWS 소유하고 관리하는 AWS KMS (AWS 키 관리 서비스) 키를 사용하여 모든 데이터를 DataZone 암호화합니다. AWS KMS로 관리하는 키를 사용하여 Amazon DataZone 카탈로그에 저장된 데이터를 암호화할 수도 있습니다.

DataZoneAmazon에서 도메인을 생성할 때 데이터 암호화에서 암호화 설정 사용자 지정 (고급) 옆의 확인란을 선택하고 KMS 키를 제공하여 암호화 설정을 제공할 수 있습니다.

전송 중 암호화

DataZone Amazon은 전송 중 암호화를 위해 전송 계층 보안 (TLS) 및 클라이언트 측 암호화를 사용합니다. Amazon과의 DataZone 통신은 항상 HTTPS를 통해 이루어지므로 전송 중에 데이터가 항상 암호화됩니다.

인터네트워크 트래픽 개인 정보 보호

계정 간 연결을 보호하기 위해 DataZone Amazon은 서비스 역할 및 IAM 역할을 사용하여 고객 계정에 안전하게 연결하고 고객을 대신하여 작업을 실행합니다.

주제

- Amazon의 유휴 데이터 암호화 DataZone
- Amazon용 인터페이스 VPC 엔드포인트 사용 DataZone

Amazon의 유휴 데이터 암호화 DataZone

저장 데이터를 기본적으로 암호화하면 민감한 데이터 보호와 관련된 운영 오버헤드와 복잡성을 줄이는 데 도움이 됩니다. 동시에 엄격한 암호화 규정 준수 및 규제 요구 사항을 충족하는 안전한 애플리케이션을 구축할 수 있습니다.

DataZone Amazon은 기본 AWS소유 키를 사용하여 저장된 데이터를 자동으로 암호화합니다. AWS 소유 키의 사용을 확인, 관리 또는 감사할 수 없습니다. 자세한 내용은 AWS 소유 키를 참조하십시오.

이 암호화 계층을 비활성화하거나 다른 암호화 유형을 선택할 수는 없지만 Amazon DataZone 도메인을 생성할 때 고객 관리 키를 선택하여 기존 AWS 소유 암호화 키 위에 두 번째 암호화 계층을 추가할 수 있습니다. Amazon은 대칭적인 고객 관리형 키를 사용할 수 있도록 DataZone 지원합니다. 이 키를

생성하여 소유하고 관리하여 기존 AWS 소유 암호화에 두 번째 암호화 계층을 추가할 수 있습니다. 이 암호화 계층을 완전히 제어할 수 있으므로 이 계층에서 다음 작업을 수행할 수 있습니다.

- 키 정책 수립 및 유지
- IAM 정책 및 보조금 수립 및 유지
- 키 정책 활성화 및 비활성화
- 주요 암호화 자료 교체
- 태그 추가
- 키 별칭 생성
- 삭제를 위한 스케줄 키

자세한 내용은 고객 관리 키를 참조하십시오.

> **Note**
>
> Amazon은 AWS 소유 키를 사용하여 저장된 데이터를 DataZone 자동으로 암호화하여 고객 데이터를 무료로 보호합니다.
> AWS 고객 관리 키 사용에는 KMS 요금이 적용됩니다. 요금에 대한 자세한 내용은 AWS 키 관리 서비스 요금을 참조하십시오.

Amazon이 AWS KMS에서 보조금을 DataZone 사용하는 방법

Amazon에서 고객 관리 키를 DataZone 사용하려면 세 가지 승인을 받아야 합니다. 고객 관리 키로 암호화된 Amazon DataZone 도메인을 생성하면 Amazon이 AWS KMS에 CreateGrant요청을 전송하여 사용자를 대신하여 권한 부여 및 하위 권한 부여를 DataZone 생성합니다. AWS KMS 보조금은 Amazon이 사용자 계정의 KMS 키에 DataZone 액세스할 수 있도록 하는 데 사용됩니다. DataZone Amazon은 고객 관리 키를 다음과 같은 내부 작업에 사용하기 위해 다음과 같은 권한을 부여합니다.

다음 작업을 위해 저장된 데이터를 암호화하는 데 사용할 수 있는 1회의 허가:

- AWS KMS에 DescribeKey요청을 보내 Amazon DataZone 도메인 컬렉션을 생성할 때 입력한 대칭 고객 관리형 KMS 키 ID가 유효한지 확인합니다.
- GenerateDataKeyrequests AWS KMS로 전송하여 고객 관리 키로 암호화된 데이터 키를 생성하십시오.
- 암호화된 데이터 키를 해독하여 데이터를 암호화하는 데 사용할 수 있도록 AWS KMS에 암호 해독 요청을 보내십시오.

- RetireGrant도메인이 삭제되면 권한 부여를 철회하기 위해서입니다.

데이터 검색 및 발견을 위한 두 가지 보조금:

- 보조금 2:
  - DescribeKey
  - GenerateDataKey
  - 암호화, 복호화, ReEncrypt
  - CreateGrant에서 내부적으로 사용하는 AWS 서비스에 대한 아동 지원금을 조성하기 위함입니다. DataZone
  - RetireGrant
- 보조금 3:
  - GenerateDataKey
  - Decrypt
  - RetireGrant

언제든지 권한 부여에 대한 액세스 권한을 취소하거나 고객 관리형 키에 대한 서비스 액세스를 제거할 수 있습니다. 이렇게 하면 Amazon은 고객 관리 키로 암호화된 데이터에 액세스할 수 DataZone 없게 되며, 이는 해당 데이터에 종속된 작업에 영향을 미칩니다. 예를 들어 Amazon이 액세스할 DataZone 수 없는 데이터 자산 세부 정보를 가져오려고 하면 작업에서 `AccessDeniedException` 오류가 반환됩니다.

고객 관리형 키 생성

AWS 관리 콘솔 또는 AWS KMS API를 사용하여 대칭 고객 관리 키를 생성할 수 있습니다.

대칭 고객 관리 키를 생성하려면 키 관리 서비스 개발자 가이드의 대칭 고객 관리 키 생성 단계를 따르세요. AWS

키 정책 - 키 정책은 고객 관리 키에 대한 액세스를 제어합니다. 모든 고객 관리형 키에는 키를 사용할 수 있는 사람과 키를 사용하는 방법을 결정하는 문장이 포함된 정확히 하나의 키 정책이 있어야 합니다. 고객 관리형 키를 생성할 때 키 정책을 지정할 수 있습니다. 자세한 내용은 키 관리 서비스 개발자 가이드의 고객 관리 키에 AWS 대한 액세스 관리를 참조하십시오.

Amazon DataZone 리소스에서 고객 관리 키를 사용하려면 키 정책에서 다음 API 작업을 허용해야 합니다.

- kms: CreateGrant — 고객 관리 키에 권한 부여를 추가합니다. 지정된 KMS 키에 대한 제어 액세스 권한을 부여하여 Amazon에서 DataZone 요구하는 작업을 허용할 수 있습니다. Grants 사용에 대한 자세한 내용은 AWS 키 관리 서비스 개발자 안내서를 참조하십시오.
- kms: DescribeKey — DataZone Amazon이 키를 검증할 수 있도록 고객 관리형 키 세부 정보를 제공합니다.
- kms: GenerateDataKey — KMS 외부에서 사용할 수 있는 고유한 대칭 데이터 키를 반환합니다. AWS
- KMS:암호 해독 — KMS 키로 암호화된 암호문을 해독합니다.

Amazon에 추가할 수 있는 정책 설명 예시는 다음과 같습니다 DataZone.

```
"Statement" : [
    {
      "Sid" : "Allow access to principals authorized to manage Amazon DataZone",
      "Effect" : "Allow",
      "Principal" : {
        "AWS" : "arn:aws:iam::<account_id>:root"
      },
      "Action" : [
        "kms:DescribeKey",
        "kms:CreateGrant",
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:region:<account_id>:key/key_ID",
    }
  ]
```

> **Note**
>
> Amazon DataZone 데이터 포털을 통해 액세스한 리소스에는 KMS 정책에 대한 거부가 적용되지 않습니다.

정책에서 권한을 지정하는 방법에 대한 자세한 내용은 AWS 키 관리 서비스 개발자 안내서를 참조하십시오.

키 액세스 문제 해결에 대한 자세한 내용은 AWS 키 관리 서비스 개발자 안내서를 참조하십시오.

Amazon의 고객 관리 키 지정 DataZone

Amazon DataZone 암호화 컨텍스트

암호화 컨텍스트는 데이터에 대한 추가 컨텍스트 정보를 포함하는 선택적 키-값 페어 세트입니다.

AWS KMS는 암호화 컨텍스트를 인증된 추가 데이터로 사용하여 인증된 암호화를 지원합니다. 데이터 암호화 요청에 암호화 컨텍스트를 포함시키면 AWS KMS는 암호화 컨텍스트를 암호화된 데이터에 바인딩합니다. 요청에 동일한 암호화 컨텍스트를 포함해야 이 데이터를 해독할 수 있습니다.

DataZone Amazon은 다음과 같은 암호화 컨텍스트를 사용합니다.

```
"encryptionContextSubset": {
    "aws:datazone:domainId": "{root-domain-uuid}"
}
```

모니터링을 위한 암호화 컨텍스트 사용 - 대칭적인 고객 관리 키를 사용하여 DataZone Amazon을 암호화하는 경우 감사 레코드 및 로그의 암호화 컨텍스트를 사용하여 고객 관리 키가 사용되는 방식을 식별할 수도 있습니다. 암호화 컨텍스트는 AWS CloudTrail 또는 Amazon Logs에서 생성한 CloudWatch 로그에도 나타납니다.

암호화 컨텍스트를 사용하여 고객 관리 키에 대한 액세스 제어 - 키 정책 및 IAM 정책의 암호화 컨텍스트를 조건으로 사용하여 대칭형 고객 관리 키에 대한 액세스를 제어할 수 있습니다. 또한 권한 부여에서 암호화 컨텍스트 제약 조건을 사용할 수 있습니다.

DataZone Amazon은 권한 부여에서 암호화 컨텍스트 제약을 사용하여 계정 또는 지역의 고객 관리 키에 대한 액세스를 제어합니다. 권한 부여 제약 조건에 따라 권한 부여가 허용하는 작업은 지정된 암호화 컨텍스트를 사용해야 합니다.

다음은 특정 암호화 컨텍스트에서 고객 관리형 키에 대한 액세스 권한을 부여하는 키 정책 설명의 예입니다. 이 정책 설명의 조건에 따라 권한 부여에는 암호화 컨텍스트를 지정하는 암호화 컨텍스트 제약 조건이 있어야 합니다.

```
{
    "Sid": "Enable DescribeKey",
    "Effect": "Allow",
    "Principal": {
```

```
        "AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"
     },
     "Action": "kms:DescribeKey",
     "Resource": "*"
},{
    "Sid": "Enable Decrypt, GenerateDataKey",
     "Effect": "Allow",
     "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"
     },
     "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
     ],
     "Resource": "*",
     "Condition": {
        "StringEquals": {
            "kms:EncryptionContext:aws:datazone:domainId": "{root-domain-uuid}"
        }
    }
}
```

Amazon의 암호화 키 모니터링 DataZone

AWS KMS 고객 관리 키를 Amazon DataZone 리소스와 함께 사용하면 Amazon이 AWS KMS에 DataZone 보내는 요청을 추적하는 AWS CloudTrail데 사용할 수 있습니다. 다음 예는 고객 관리 키로 암호화된 데이터에 `DescribeKey` 액세스하기 위해 Amazon에서 호출하는 `CreateGrant` `GenerateDataKeyDecrypt`,, 및 KMS 작업을 DataZone 모니터링하기 위한 AWS CloudTrail 이벤트입니다. AWS KMS 고객 관리 키를 사용하여 Amazon DataZone 도메인을 암호화하면 Amazon이 사용자 대신 사용자 계정의 KMS 키에 액세스해 `CreateGrant` 달라는 요청을 DataZone 보냅니다. AWS Amazon에서 DataZone 생성하는 권한 부여는 AWS KMS 고객 관리 키와 관련된 리소스에만 적용됩니다. 또한 DataZone Amazon은 도메인을 삭제할 때 이 `RetireGrant` 작업을 사용하여 권한 부여를 제거합니다. 다음 예제 이벤트는 `CreateGrant` 작업을 기록합니다.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
```

```
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-04-22T17:02:00Z"
            }
        },
        "invokedBy": "datazone.amazonaws.com"
    },
    "eventTime": "2021-04-22T17:07:02Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "172.12.34.56",
    "userAgent": "ExampleDesktop/1.0 (V1; OS)",
    "requestParameters": {
        "constraints": {
            "encryptionContextSubset": {
                "aws:datazone:domainId": "SAMPLE-root-domain-uuid"
            }
        },
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "operations": [
            "Decrypt",
            "GenerateDataKey",
            "RetireGrant",
            "DescribeKey"
        ],
        "granteePrincipal": "datazone.us-west-2.amazonaws.com"
    },
    "responseElements": {
        "grantId":
 "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE",
```

```
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
}
```

암호화된 AWS Glue 카탈로그를 포함하는 Data Lake 환경 생성

고급 사용 사례에서는 암호화된 AWS Glue 카탈로그를 사용할 때 Amazon DataZone 서비스에 대한 액세스 권한을 부여해야 고객 관리형 KMS 키를 사용할 수 있습니다. 사용자 지정 KMS 정책을 업데이트하고 키에 태그를 추가하면 이 작업을 수행할 수 있습니다. 암호화된 AWS Glue 카탈로그의 데이터로 작업할 수 있도록 Amazon DataZone 서비스에 대한 액세스 권한을 부여하려면 다음을 완료하십시오.

- 사용자 지정 KMS 키에 다음 정책을 추가합니다. 자세한 내용은 키 정책 변경을 참조하세요.

```
{
  "Sid": "Allow datazone environment roles to use the key",
  "Effect": "Allow",
  "Principal": {
    "AWS": "*"
  },
  "Action": [
    "kms:Decrypt",
    "kms:Describe*",
    "kms:Get*"
```

```
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "aws:PrincipalArn": "arn:aws:iam::*:role/*datazone_usr*"
    }
  }
}
```

- 사용자 지정 KMS 키에 다음 태그를 추가합니다. 자세한 내용은 태그를 사용하여 KMS 키에 대한 액세스 제어를 참조하십시오.

```
key: AmazonDataZoneEnvironment
value: all
```

Amazon용 인터페이스 VPC 엔드포인트 사용 DataZone

Amazon VPC (Virtual Private Cloud) 를 사용하여 AWS 리소스를 호스팅하는 경우, Amazon VPC와 Amazon 간에 연결을 설정할 수 있습니다. DataZone 퍼블릭 인터넷을 DataZone 거치지 않고도 Amazon과 이 연결을 사용할 수 있습니다.

Amazon VPC를 사용하면 사용자 지정 가상 네트워크에서 AWS 리소스를 시작할 수 있습니다. VPC를 사용하여 IP 주소 범위, 서브넷, 라우팅 테이블, 네트워크 게이트웨이 등의 네트워크 설정을 제어할 수 있습니다. VPC에 대한 자세한 내용은 Amazon VPC 사용 설명서를 참조하세요.

Amazon VPC를 Amazon에 연결하려면 먼저 VPC를 다른 서비스에 연결할 수 있는 인터페이스 VPC 엔드포인트를 정의해야 합니다. DataZone AWS 이 엔드포인트를 이용하면 인터넷 게이트웨이나 NAT(네트워크 주소 변환) 인스턴스 또는 VPN 연결 없이도 안정적이고 확장 가능하게 연결됩니다. VPC 엔드포인트를 생성하는 방법에 대한 자세한 내용 및 세부 단계는 Amazon VPC 사용 설명서의 인터페이스 VPC 엔드포인트 ()AWS PrivateLink 를 참조하십시오.

> **Important**
>
> VPC에서 엔드포인트 정책은 VPC 엔드포인트에 연결하여 엔드포인트를 사용하여 서비스에 액세스할 수 있는 AWS 보안 주체를 제어할 수 있는 리소스 기반 정책입니다. AWS

Amazon의 현재 DataZone 릴리스에서는 Amazon VPC와 Amazon 간의 연결 설정 및 사용에 대한 엔드포인트 정책 사용이 지원되지 않습니다. DataZone Amazon DataZone 액세스 관리는 서비스 수준에서 정의된 RAM 구성 및 IAM 기본 정책을 기반으로 합니다.

아마존에서의 인증 DataZone

DataZoneAmazon의 인터페이스는 콘솔 내 관리 AWS 콘솔과 콘솔 외부의 웹 애플리케이션 (데이터 포털) 으로 구성되어 있습니다.

AWS 관리자는 도메인 생성 및 DataZone 관리, 해당 도메인에 대한 AWS 계정 연결, Amazon에 액세스 관리를 위임하려는 데이터 소스를 비롯한 top-level-resource API에 대해 Amazon 관리 콘솔을 사용할 수 있습니다. DataZone Amazon DataZone 관리 콘솔을 사용하여 명시적으로 구성된 계정에 대한 액세스 관리 제어를 Amazon DataZone 서비스에 위임하는 데 필요한 모든 IAM 역할 및 구성을 관리할 수 있습니다. AWS Amazon DataZone 데이터 포털은 SSO 사용자를 위한 퍼스트 파티 AWS ID 센터 애플리케이션입니다. 활성화된 경우 인증된 IAM 보안 주체가 SSO ID를 사용하는 대신 콘솔을 사용하여 데이터 포털에 페더레이션할 수도 있습니다.

DataZoneAmazon의 데이터 포털은 주로 AWS IAM Identity Center 인증을 받은 사용자가 데이터 액세스를 관리하고 데이터 게시, 검색, 구독 및 분석 작업을 수행하는 데 사용하도록 설계되었습니다.

Amazon DataZone 콘솔에서의 권한 부여

Amazon DataZone 콘솔 인증 모델은 IAM 인증을 사용합니다. 콘솔은 관리자가 주로 설정용으로 사용합니다. DataZone Amazon은 도메인 관리자 AWS 계정과 멤버 AWS 계정이라는 개념을 사용하며 이러한 모든 계정에서 콘솔을 사용하여 AWS 조직의 경계를 존중하면서 신뢰 관계를 구축합니다.

Amazon DataZone 포털에서의 인증

Amazon DataZone 데이터 포털 인증 모델은 관리자와 최종 사용자를 포함하는 정적 역할 원형 (프로필) 이 있는 계층적 ACL입니다. 예를 들어 사용자는 관리자 또는 사용자 프로필을 가질 수 있습니다. 도메인 수준에서는 도메인 사용자를 데이터 소유자로 지정할 수 있습니다. 프로젝트 수준에서 사용자는 소유자 또는 기여자가 될 수 있습니다. 이러한 프로필은 사용자와 그룹의 두 가지 유형 중 하나로 구성할 수 있습니다. 그러면 이러한 프로필이 도메인 및 프로젝트와 연결되고 이러한 권한의 상태가 연결 테이블에 저장됩니다.

Amazon은 이 인증 모델 내에서 사용자가 사용자 및 그룹 권한을 관리할 DataZone 수 있도록 허용합니다. 사용자는 프로젝트 멤버십을 관리하고, 프로젝트 멤버십을 요청하고, 멤버십을 승인합니다. 사용자는 데이터를 게시하고, 데이터 구독 승인자를 정의하고, 데이터를 구독하고, 구독을 승인합니다.

사용자는 데이터 포털 클라이언트가 IAM 세션 자격 증명을 요청하면 특정 프로젝트에서 데이터 분석을 수행합니다. 이 자격 증명은 Amazon이 특정 프로젝트 컨텍스트에서 사용자의 유효 프로필을 기반으로 DataZone 생성합니다. 이 세션의 범위는 사용자 권한과 특정 프로젝트 리소스 모두에 적용됩니다. 그런 다음 사용자가 Athena 또는 Redshift로 이동하여 관련 데이터를 쿼리하면 모든 기본 IAM 작업이 완전히 추상화됩니다.

아마존 DataZone 프로필 및 역할

사용자가 인증되면 인증된 컨텍스트가 사용자 프로필 ID에 매핑됩니다. 이 사용자 프로필에는 사용자 권한 부여에 사용되는 여러 개의 서로 다른 연결 (프로젝트 소유자, 도메인 관리자 등) 이 있을 수 있습니다. 각 연결 (예: 프로젝트 소유자, 도메인 관리자 등) 은 컨텍스트에 따라 특정 활동에 대한 권한을 가집니다. 예를 들어 도메인 관리자 연결이 있는 사용자는 추가 도메인을 작성하고, 도메인에 다른 도메인 관리자를 할당하고, 해당 도메인 내에 프로젝트 템플릿을 작성할 수 있습니다. 프로젝트 소유자는 프로젝트에 프로젝트 멤버를 추가 또는 제거하고, 도메인과 게시 계약을 체결하고, 도메인에 자산을 게시할 수 있습니다.

IAM을 사용하여 Amazon DataZone 리소스에 대한 액세스 제어

다음 보안 관련 작업을 완료하려면 AWS Identity and Access Management (IAM) 이 필요합니다.

- 아래에서 사용자 및 그룹을 생성하십시오. AWS 계정
- 소속된 각 사용자에게 고유한 보안 자격 증명을 할당하십시오 AWS 계정.
- AWS 리소스로 작업을 수행할 수 있는 각 사용자의 권한을 제어하세요.
- 다른 사용자의 AWS 리소스 AWS 계정 공유를 허용하세요.
- 역할을 생성하고 역할을 맡을 수 있는 사용자 또는 서비스를 정의하세요 AWS 계정 .
- 기업의 기존 ID를 사용하여 리소스를 사용하여 AWS 작업을 수행할 수 있는 권한을 부여하십시오.

IAM에 대한 자세한 내용은 다음을 참조하십시오.

- AWS Identity and Access Management (IAM)
- 시작하기
- IAM 사용 설명서

다음 섹션에서는 도메인 (도메인 포함), 관련 계정, 프로젝트, 데이터 소스 등 Amazon DataZone 및 해당 구성 요소를 설정하는 데 필요한 정책 및 권한을 설명합니다. 자세한 내용은 아마존 DataZone 용어 및 개념 단원을 참조하십시오.

목차

AWS 아마존 관리형 정책 DataZone

AWS 관리형 정책은 에서 생성하고 관리하는 독립형 정책입니다. AWS AWS 관리형 정책은 많은 일반 사용 사례에 대한 권한을 제공하도록 설계되었으므로 사용자, 그룹 및 역할에 권한을 할당하기 시작할 수 있습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있으므로 특정 사용 사례에 대해 최소 권한 권한을 부여하지 않을 수도 있다는 점에 유의하세요. 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다.

관리형 정책에 정의된 권한은 변경할 수 없습니다. AWS AWS 관리형 정책에 정의된 권한을 업데이트하는 경우 AWS 해당 업데이트는 정책이 연결된 모든 주체 ID (사용자, 그룹, 역할) 에 영향을 미칩니다. AWS 새 API 작업이 시작되거나 기존 서비스에 새 AWS 서비스 API 작업을 사용할 수 있게 되면 AWS 관리형 정책을 업데이트할 가능성이 가장 높습니다.

자세한 내용은 IAM 사용자 설명서의 AWS 관리형 정책을 참조하세요.

내용

- AWS 관리형 정책: AmazonDataZoneSageMakerAccess
- AWS 관리형 정책: AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary
- Amazon, AWS 관리형 정책 DataZone 업데이트

AWS 관리형 정책: AmazonDataZoneFullAccess

`AmazonDataZoneFullAccess` 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책은 DataZone 를 통해 Amazon에 대한 전체 액세스를 제공합니다 AWS Management Console.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `datazone`— 주도자에게 를 DataZone 통해 Amazon에 대한 전체 액세스 권한을 부여합니다. AWS Management Console
- `kms`— 보안 주체가 별칭을 나열하고 키를 설명할 수 있습니다.
- `s3`— 보안 주체가 Amazon 데이터를 저장할 기존 S3 버킷을 선택하거나 새 S3 버킷을 생성할 수 있습니다. DataZone
- `ram`— 보안 주체가 Amazon DataZone 도메인을 공유할 수 있습니다. AWS 계정
- `iam`— 보안 주체가 역할을 나열하고 전달하며 정책을 가져올 수 있습니다.
- `sso`— 주도자가 활성화된 지역을 가져올 수 있습니다. AWS IAM Identity Center

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AmazonDataZoneStatement",
      "Effect": "Allow",
      "Action": [
        "datazone:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "ReadOnlyStatement",
```

```
      "Effect": "Allow",
      "Action": [
        "kms:DescribeKey",
        "kms:ListAliases",
        "iam:ListRoles",
        "sso:DescribeRegisteredRegions",
        "s3:ListAllMyBuckets",
        "redshift:DescribeClusters",
        "redshift-serverless:ListWorkgroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "secretsmanager:ListSecrets"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "BucketReadOnlyStatement",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Sid": "CreateBucketStatement",
      "Effect": "Allow",
      "Action": "s3:CreateBucket",
      "Resource": "arn:aws:s3:::amazon-datazone*"
    },
    {
      "Sid": "RamCreateResourceStatement",
      "Effect": "Allow",
      "Action": [
        "ram:CreateResourceShare"
      ],
      "Resource": "*",
      "Condition": {
        "StringEqualsIfExists": {
          "ram:RequestedResourceType": "datazone:Domain"
        }
```

```
      }
    },
    {
      "Sid": "RamResourceStatement",
      "Effect": "Allow",
      "Action": [
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:RejectResourceShareInvitation"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "ram:ResourceShareName": [
            "DataZone*"
          ]
        }
      }
    },
    {
      "Sid": "RamResourceReadOnlyStatement",
      "Effect": "Allow",
      "Action": [
        "ram:GetResourceShares",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations"
      ],
      "Resource": "*"
    },
    {
      "Sid": "IAMPassRoleStatement",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": [
        "arn:aws:iam::*:role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonDataZone*"
      ],
      "Condition": {
        "StringEquals": {
          "iam:passedToService": "datazone.amazonaws.com"
        }
      }
    },
```

```
    {
      "Sid": "IAMGetPolicyStatement",
      "Effect": "Allow",
      "Action": "iam:GetPolicy",
      "Resource": [
        "arn:aws:iam::*:policy/service-role/AmazonDataZoneRedshiftAccessPolicy*"
      ]
    },
    {
      "Sid": "DataZoneTagOnCreate",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:TagResource"
      ],
      "Resource": "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition": {
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "AmazonDataZoneDomain"
          ]
        },
        "StringLike": {
          "aws:RequestTag/AmazonDataZoneDomain": "dzd_*",
          "aws:ResourceTag/AmazonDataZoneDomain": "dzd_*"
        },
        "Null": {
          "aws:TagKeys": "false"
        }
      }
    },
    {
      "Sid": "CreateSecretStatement",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:CreateSecret"
      ],
      "Resource": "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition": {
        "StringLike": {
          "aws:RequestTag/AmazonDataZoneDomain": "dzd_*"
        }
      }
    }
  ]
```

```
}
```

정책 고려 사항 및 제한

AmazonDataZoneFullAccess정책에서 다루지 않는 특정 기능이 있습니다.

- 자체 AWS KMS 키로 Amazon DataZone 도메인을 생성하는 경우 도메인 DataZone 생성이 성공하고 해당 키가 및 등의 listDataSources 다른 Amazon API를 호출할 수 있는 권한이 있어야 합니다. kms:CreateGrant kms:GenerateDataKey kms:Decrypt createDataSource 또한 해당 키의kms:CreateGrant, kms:Decryptkms:GenerateDataKey, 및 kms:DescribeKey 리소스 정책에 대한 권한도 있어야 합니다.

  기본 서비스 소유 KMS 키를 사용하는 경우에는 이 키가 필요하지 않습니다.

  자세한 정보는 AWS Key Management Service을 참조하세요.
- Amazon DataZone 콘솔 내에서 역할 생성 및 업데이트 기능을 사용하려면 관리자 권한이 있거나 IAM 역할을 생성하고 정책을 생성/업데이트하는 데 필요한 IAM 권한이 있어야 합니다. 필수 권한에는iam:CreateRole,,, iam:CreatePolicy 권한이 포함됩니다. iam:CreatePolicyVersion iam:DeletePolicyVersion iam:AttachRolePolicy
- AWS IAM Identity Center 사용자 로그인이 활성화된 상태로 DataZone Amazon에서 새 도메인을 생성하거나 Amazon의 기존 도메인에 대해 도메인을 활성화하는 경우 DataZone sso:CreateManagedApplicationInstancesso:DeleteManagedApplicationInstance, 및 에 대한 권한이 있어야 합니다sso:PutApplicationAssignmentConfiguration.
- DataZoneAmazon에서 AWS 계정 연결 요청을 수락하려면 ram:AcceptResourceShareInvitation 권한이 있어야 합니다.

AWS 관리형 정책: AmazonDataZoneFullUserAccess

이 정책은 DataZone Amazon에 대한 전체 액세스 권한을 부여하지만 도메인, 사용자 또는 관련 계정의 관리는 허용하지 않습니다.

권한 세부 정보

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AmazonDataZoneUserOperations",
```

```
      "Effect": "Allow",
      "Action": [
        "datazone:GetDomain",
        "datazone:CreateFormType",
        "datazone:GetFormType",
        "datazone:GetIamPortalLoginUrl",
        "datazone:SearchUserProfiles",
        "datazone:SearchGroupProfiles",
        "datazone:GetUserProfile",
        "datazone:GetGroupProfile",
        "datazone:ListGroupsForUser",
        "datazone:DeleteFormType",
        "datazone:CreateAssetType",
        "datazone:GetAssetType",
        "datazone:DeleteAssetType",
        "datazone:CreateGlossary",
        "datazone:GetGlossary",
        "datazone:DeleteGlossary",
        "datazone:UpdateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:GetGlossaryTerm",
        "datazone:DeleteGlossaryTerm",
        "datazone:UpdateGlossaryTerm",
        "datazone:CreateAsset",
        "datazone:GetAsset",
        "datazone:DeleteAsset",
        "datazone:CreateAssetRevision",
        "datazone:ListAssetRevisions",
        "datazone:AcceptPredictions",
        "datazone:RejectPredictions",
        "datazone:Search",
        "datazone:SearchTypes",
        "datazone:CreateListingChangeSet",
        "datazone:DeleteListing",
        "datazone:SearchListings",
        "datazone:GetListing",
        "datazone:CreateDataSource",
        "datazone:GetDataSource",
        "datazone:DeleteDataSource",
        "datazone:UpdateDataSource",
        "datazone:ListDataSources",
        "datazone:StartDataSourceRun",
        "datazone:GetDataSourceRun",
        "datazone:ListDataSourceRuns",
```

```
        "datazone:ListDataSourceRunActivities",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:CreateEnvironmentBlueprint",
        "datazone:GetEnvironmentBlueprint",
        "datazone:DeleteEnvironmentBlueprint",
        "datazone:UpdateEnvironmentBlueprint",
        "datazone:ListEnvironmentBlueprints",
        "datazone:CreateProject",
        "datazone:UpdateProject",
        "datazone:GetProject",
        "datazone:DeleteProject",
        "datazone:ListProjects",
        "datazone:CreateProjectMembership",
        "datazone:DeleteProjectMembership",
        "datazone:ListProjectMemberships",
        "datazone:CreateEnvironmentProfile",
        "datazone:GetEnvironmentProfile",
        "datazone:UpdateEnvironmentProfile",
        "datazone:DeleteEnvironmentProfile",
        "datazone:ListEnvironmentProfiles",
        "datazone:CreateEnvironment",
        "datazone:GetEnvironment",
        "datazone:DeleteEnvironment",
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:ListEnvironments",
        "datazone:ListAccountEnvironments",
        "datazone:GetEnvironmentActionLink",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetSubscriptionTarget",
        "datazone:DeleteSubscriptionTarget",
        "datazone:ListSubscriptionTargets",
        "datazone:CreateSubscriptionRequest",
        "datazone:AcceptSubscriptionRequest",
        "datazone:UpdateSubscriptionRequest",
        "datazone:ListWarehouseMetadata",
        "datazone:RejectSubscriptionRequest",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:ListSubscriptionRequests",
        "datazone:DeleteSubscriptionRequest",
        "datazone:GetSubscription",
        "datazone:CancelSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:ListSubscriptions",
```

```
        "datazone:RevokeSubscription",
        "datazone:CreateSubscriptionGrant",
        "datazone:DeleteSubscriptionGrant",
        "datazone:GetSubscriptionGrant",
        "datazone:ListSubscriptionGrants",
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:ListNotifications",
        "datazone:StartMetadataGenerationRun",
        "datazone:GetMetadataGenerationRun",
        "datazone:CancelMetadataGenerationRun",
        "datazone:ListMetadataGenerationRuns"
      ],
      "Resource": "*"
    },
    {
      "Sid": "RAMResourceShareOperations",
      "Effect": "Allow",
      "Action": "ram:GetResourceShareAssociations",
      "Resource": "*"
    }
  ]
}
```

AWS 관리형 정책: AmazonDataZoneCustomEnvironmentDeploymentPolicy

이 정책을 사용하여 사용자 지정 블루프린트를 사용하여 만든 환경의 구성을 업데이트할 수 있습니다. 이 정책을 사용하여 Amazon DataZone 구독 대상 및 데이터 소스를 생성할 수도 있습니다.

권한 세부 정보

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AmazonDataZoneCustomEnvironment",
   "Effect": "Allow",
   "Action": [
    "datazone:ListAssociatedAccounts",
    "datazone:GetAccountAssociation",
    "datazone:GetEnvironment",
    "datazone:GetEnvironmentProfile",
```

```
    "datazone:GetEnvironmentBlueprint",
    "datazone:GetProject",
    "datazone:UpdateEnvironmentConfiguration",
    "datazone:UpdateEnvironmentDeploymentStatus",
    "datazone:CreateSubscriptionTarget",
    "datazone:CreateDataSource"
   ],
   "Resource": "*"
  }
 ]
}
```

AWS 관리형 정책: AmazonDataZoneEnvironmentRolePermissionsBoundary

> **Note**
>
> 이 정책은 권한 경계입니다. 권한 경계는 ID 기반 정책이 IAM 개체에 부여할 수 있는 최대 권한을 설정합니다. Amazon DataZone 권한 경계 정책을 직접 사용하고 첨부해서는 안 됩니다. Amazon DataZone 권한 경계 정책은 Amazon DataZone 관리 역할에만 연결해야 합니다. 권한 경계에 대한 자세한 내용은 IAM 사용 설명서의 IAM 엔티티의 권한 경계를 참조하십시오.

Amazon DataZone 데이터 포털을 통해 환경을 생성하면 Amazon은 환경 생성 중에 생성되는 IAM 역할에 이 권한 경계를 DataZone 적용합니다. 권한 경계는 Amazon이 DataZone 생성하는 역할 및 사용자가 추가하는 모든 역할의 범위를 제한합니다.

DataZone Amazon은 `AmazonDataZoneEnvironmentRolePermissionsBoundary` 관리형 정책을 사용하여 연결된 프로비저닝된 IAM 보안 주체를 제한합니다. 보안 주체는 Amazon이 대화형 엔터프라이즈 사용자 또는 분석 서비스 (예:) 를 대신하여 맡을 DataZone 수 있는 사용자 역할의 형태를 취하고 AWS Glue, Amazon S3에서 읽기 및 쓰기 또는 실행과 같은 데이터 처리 작업을 수행할 수 있습니다. AWS Glue 크롤러

이 `AmazonDataZoneEnvironmentRolePermissionsBoundary` 정책은 Amazon에 Amazon S3 AWS Glue, Amazon DataZone Redshift 및 Amazon Athena와 같은 서비스에 읽기 및 쓰기 액세스 권한을 부여합니다. AWS Lake Formation또한 이 정책은 이러한 서비스를 사용하는 데 필요한 일부 인프라 리소스 (예: 네트워크 인터페이스 및 키) 에 읽기 및 AWS KMS 쓰기 권한을 부여합니다.

Amazon은 AmazonDataZoneEnvironmentRolePermissionsBoundary AWS 관리형 정책을 모든 Amazon DataZone 환경 역할 (소유자 및 기여자) 에 대한 권한 경계로 DataZone 적용합니다. 이 권한 경계는 환경에 필요한 리소스 및 작업에 대한 액세스만 허용하도록 이러한 역할을 제한합니다.

경계에는 다음과 같은 JSON 명령문이 포함됩니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateGlueConnection",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition": {
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "aws-glue-service-resource"
          ]
        }
      }
    },
    {
      "Sid": "GlueOperations",
      "Effect": "Allow",
      "Action": [
        "glue:*DataQuality*",
        "glue:BatchCreatePartition",
        "glue:BatchDeleteConnection",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:BatchStopJobRun",
        "glue:BatchUpdatePartition",
        "glue:CreateBlueprint",
```

```
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDatabase",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteBlueprint",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeleteConnection",
        "glue:DeleteCrawler",
        "glue:DeleteJob",
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:DeleteWorkflow",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:ListSchemas",
        "glue:ListJobs",
        "glue:NotifyEvent",
        "glue:PutWorkflowRunProperties",
        "glue:ResetJobBookmark",
        "glue:ResumeWorkflowRun",
        "glue:SearchTables",
        "glue:StartBlueprintRun",
        "glue:StartCrawler",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:StopCrawler",
        "glue:StopCrawlerSchedule",
        "glue:StopWorkflowRun",
        "glue:UpdateBlueprint",
```

```
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateConnection",
        "glue:UpdateCrawler",
        "glue:UpdateCrawlerSchedule",
        "glue:UpdateDatabase",
        "glue:UpdateJob",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:UpdateWorkflow"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
        }
      }
    },
    {
      "Sid": "PassRole",
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid": "SameAccountKmsOperations",
      "Effect": "Allow",
      "Action": [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
```

```
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "KmsOperationsWithResourceTag",
      "Effect": "Allow",
      "Action": [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:Verify",
        "kms:Sign"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
        }
      }
    },
    {
      "Sid": "AnalyticsOperations",
      "Effect": "Allow",
      "Action": [
        "datazone:*",
        "sqlworkbench:*"
      ],
      "Resource": "*"
    },
    {
      "Sid": "QueryOperations",
      "Effect": "Allow",
      "Action": [
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
```

```
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:Describe*",
        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetJobs",
        "glue:BatchGetPartition",
        "glue:BatchGetWorkflows",
        "glue:BatchUpdatePartition",
        "glue:CreateBlueprint",
```

```
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDatabase",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:ListSchemas",
        "glue:ListJobs",
        "glue:NotifyEvent",
        "glue:SearchTables",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateDatabase",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListGroups",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListUsers",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeMetricFilters",
```

```
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetLogEvents",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:GetLogRecord",
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:FilterLogEvents",
        "lakeformation:GetDataAccess",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListPermissions",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable",
        "redshift-data:ListSchemas",
        "redshift-data:ListDatabases",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift:CreateClusterUser",
        "redshift:DescribeClusters",
        "redshift:DescribeDataShares",
        "redshift:GetClusterCredentials",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:JoinGroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetCredentials",
        "secretsmanager:ListSecrets",
        "tag:GetResources"
      ],
      "Resource": "*"
    },
    {
      "Sid": "QueryOperationsWithResourceTag",
      "Effect": "Allow",
      "Action": [
        "athena:GetQueryResultsStream"
      ],
      "Resource": "*",
      "Condition": {
```

```
        "Null": {
          "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
        }
      }
    },
    {
      "Sid": "SecretsManagerOperationsWithTagKeys",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource": "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/AmazonDataZoneDomain": "*",
          "aws:ResourceTag/AmazonDataZoneProject": "*"
        },
        "Null": {
          "aws:TagKeys": "false"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "AmazonDataZoneDomain",
            "AmazonDataZoneProject"
          ]
        }
      }
    },
    {
      "Sid": "DataZoneS3Buckets",
      "Effect": "Allow",
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObject",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject"
      ],
      "Resource": [
        "arn:aws:s3:::*/datazone/*"
```

```
      ]
    },
    {
      "Sid": "DataZoneS3BucketLocation",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ListDataZoneS3Bucket",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringLike": {
          "s3:prefix": [
            "*/datazone/*",
            "datazone/*"
          ]
        }
      }
    },
    {
      "Sid": "NotDeniedOperations",
      "Effect": "Deny",
      "NotAction": [
        "datazone:*",
        "sqlworkbench:*",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
```

```
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement",
        "ec2:CreateNetworkInterface",
        "ec2:CreateTags",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteTags",
        "ec2:Describe*",
        "glue:*DataQuality*",
        "glue:BatchCreatePartition",
        "glue:BatchDeleteConnection",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetJobs",
        "glue:BatchGetPartition",
```

```
        "glue:BatchGetWorkflows",
        "glue:BatchStopJobRun",
        "glue:BatchUpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDatabase",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteBlueprint",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeleteConnection",
        "glue:DeleteCrawler",
        "glue:DeleteJob",
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:DeleteWorkflow",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:ListSchemas",
        "glue:ListJobs",
        "glue:NotifyEvent",
        "glue:PutWorkflowRunProperties",
        "glue:ResetJobBookmark",
        "glue:ResumeWorkflowRun",
        "glue:SearchTables",
        "glue:StartBlueprintRun",
        "glue:StartCrawler",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
```

```
        "glue:StopCrawler",
        "glue:StopCrawlerSchedule",
        "glue:StopWorkflowRun",
        "glue:UpdateBlueprint",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateConnection",
        "glue:UpdateCrawler",
        "glue:UpdateCrawlerSchedule",
        "glue:UpdateDatabase",
        "glue:UpdateJob",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:UpdateWorkflow",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:List*",
        "iam:PassRole",
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:ListKeys",
        "kms:Verify",
        "kms:Sign",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetLogEvents",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:GetLogRecord",
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:FilterLogEvents",
        "lakeformation:GetDataAccess",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListPermissions",
        "redshift-data:ListTables",
```

```
        "redshift-data:DescribeTable",
        "redshift-data:ListSchemas",
        "redshift-data:ListDatabases",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift:CreateClusterUser",
        "redshift:DescribeClusters",
        "redshift:DescribeDataShares",
        "redshift:GetClusterCredentials",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:JoinGroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetCredentials",
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject",
        "secretsmanager:CreateSecret",
        "secretsmanager:ListSecrets",
        "secretsmanager:TagResource",
        "tag:GetResources"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

AWS 관리형 정책: AmazonDataZoneRedshiftGlueProvisioningPolicy

이 AmazonDataZoneRedshiftGlueProvisioningPolicy 정책은 DataZone Amazon에 AWS Glue 및 Amazon Redshift와 상호 운용하는 데 필요한 권한을 부여합니다.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AmazonDataZonePermissionsToCreateEnvironmentRole",
   "Effect": "Allow",
   "Action": [
    "iam:CreateRole",
    "iam:DetachRolePolicy",
    "iam:DeleteRolePolicy",
    "iam:AttachRolePolicy",
    "iam:PutRolePolicy"
   ],
   "Resource": "arn:aws:iam::*:role/datazone*",
   "Condition": {
    "StringEquals": {
     "iam:PermissionsBoundary": "arn:aws:iam::aws:policy/
AmazonDataZoneEnvironmentRolePermissionsBoundary",
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "IamPassRolePermissions",
   "Effect": "Allow",
   "Action": [
    "iam:PassRole"
   ],
   "Resource": [
    "arn:aws:iam::*:role/datazone*"
   ],
   "Condition": {
    "StringEquals": {
```

```
      "iam:PassedToService": [
       "glue.amazonaws.com",
       "lakeformation.amazonaws.com"
      ],
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AmazonDataZonePermissionsToManageCreatedEnvironmentRole",
    "Effect": "Allow",
    "Action": [
     "iam:DeleteRole",
     "iam:GetRole"
    ],
    "Resource": "arn:aws:iam::*:role/datazone*",
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AmazonDataZoneCFStackCreationForEnvironments",
    "Effect": "Allow",
    "Action": [
     "cloudformation:CreateStack",
     "cloudformation:TagResource"
    ],
    "Resource": [
     "arn:aws:cloudformation:*:*:stack/DataZone*"
    ],
    "Condition": {
     "ForAnyValue:StringLike": {
      "aws:TagKeys": "AmazonDataZoneEnvironment"
     },
     "Null": {
      "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
     }
    }
```

```
  },
  {
   "Sid": "AmazonDataZoneCFStackManagementForEnvironments",
   "Effect": "Allow",
   "Action": [
    "cloudformation:DeleteStack",
    "cloudformation:DescribeStacks",
    "cloudformation:DescribeStackEvents"
   ],
   "Resource": [
    "arn:aws:cloudformation:*:*:stack/DataZone*"
   ]
  },
  {
   "Sid": "AmazonDataZoneEnvironmentParameterValidation",
   "Effect": "Allow",
   "Action": [
    "lakeformation:GetDataLakeSettings",
    "lakeformation:PutDataLakeSettings",
    "lakeformation:RevokePermissions",
    "lakeformation:ListPermissions",
    "glue:CreateDatabase",
    "glue:GetDatabase",
    "athena:GetWorkGroup",
    "logs:DescribeLogGroups",
    "redshift-serverless:GetNamespace",
    "redshift-serverless:GetWorkgroup",
    "redshift:DescribeClusters",
    "secretsmanager:ListSecrets"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AmazonDataZoneEnvironmentLakeFormationPermissions",
   "Effect": "Allow",
   "Action": [
    "lakeformation:RegisterResource",
    "lakeformation:DeregisterResource",
    "lakeformation:GrantPermissions",
    "lakeformation:ListResources"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
```

```
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AmazonDataZoneEnvironmentGlueDeletePermissions",
    "Effect": "Allow",
    "Action": [
     "glue:DeleteDatabase"
    ],
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AmazonDataZoneEnvironmentAthenaDeletePermissions",
    "Effect": "Allow",
    "Action": [
     "athena:DeleteWorkGroup"
    ],
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AmazonDataZoneEnvironmentAthenaResourceCreation",
    "Effect": "Allow",
    "Action": [
     "athena:CreateWorkGroup",
     "athena:TagResource",
     "iam:TagRole",
     "iam:TagPolicy",
```

```
    "logs:TagLogGroup"
   ],
   "Resource": "*",
   "Condition": {
    "ForAnyValue:StringLike": {
     "aws:TagKeys": "AmazonDataZoneEnvironment"
    },
    "Null": {
     "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
    },
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AmazonDataZoneEnvironmentLogGroupCreation",
   "Effect": "Allow",
   "Action": [
    "logs:CreateLogGroup",
    "logs:DeleteLogGroup"
   ],
   "Resource": "arn:aws:logs:*:*:log-group:datazone-*",
   "Condition": {
    "ForAnyValue:StringLike": {
     "aws:TagKeys": "AmazonDataZoneEnvironment"
    },
    "Null": {
     "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
    },
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AmazonDataZoneEnvironmentLogGroupManagement",
   "Action": [
    "logs:PutRetentionPolicy"
   ],
```

```
    "Resource": "arn:aws:logs:*:*:log-group:datazone-*",
    "Effect": "Allow",
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AmazonDataZoneEnvironmentIAMPolicyManagement",
    "Effect": "Allow",
    "Action": [
     "iam:DeletePolicy",
     "iam:CreatePolicy",
     "iam:GetPolicy",
     "iam:ListPolicyVersions"
    ],
    "Resource": [
     "arn:aws:iam::*:policy/datazone*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AmazonDataZoneEnvironmentS3ValidationPermissions",
    "Effect": "Allow",
    "Action": [
     "s3:ListAllMyBuckets",
     "s3:ListBucket"
    ],
    "Resource": "arn:aws:s3:::*"
   },
   {
    "Sid": "AmazonDataZoneEnvironmentKMSDecryptPermissions",
    "Effect": "Allow",
    "Action": [
     "kms:GenerateDataKey",
```

```
    "kms:Decrypt"
   ],
   "Resource": "*",
   "Condition": {
    "Null": {
     "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
    }
   }
  },
  {
   "Sid": "PermissionsToTagAmazonDataZoneEnvironmentGlueResources",
   "Effect": "Allow",
   "Action": [
    "glue:TagResource"
   ],
   "Resource": "*",
   "Condition": {
    "ForAnyValue:StringLike": {
     "aws:TagKeys": "AmazonDataZoneEnvironment"
    },
    "Null": {
     "aws:RequestTag/AmazonDataZoneEnvironment": "false"
    }
   }
  },
  {
   "Sid": "PermissionsToGetAmazonDataZoneEnvironmentBlueprintTemplates",
   "Effect": "Allow",
   "Action": "s3:GetObject",
   "Resource": "*",
   "Condition": {
    "StringNotEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    },
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "RedshiftDataPermissions",
   "Effect": "Allow",
```

```
    "Action": [
     "redshift-data:ListSchemas",
     "redshift-data:ExecuteStatement"
    ],
    "Resource": [
     "arn:aws:redshift-serverless:*:*:workgroup/*",
     "arn:aws:redshift:*:*:cluster:*"
    ]
   },
   {
    "Sid": "DescribeStatementPermissions",
    "Effect": "Allow",
    "Action": [
     "redshift-data:DescribeStatement"
    ],
    "Resource": "*"
   },
   {
    "Sid": "GetSecretValuePermissions",
    "Effect": "Allow",
    "Action": [
     "secretsmanager:GetSecretValue"
    ],
    "Resource": "*",
    "Condition": {
     "StringLike": {
      "secretsmanager:ResourceTag/AmazonDataZoneDomain": "dzd*"
     }
    }
   }
  ]
}
```

AWS 관리형 정책: AmazonDataZoneGlueManageAccessRolePolicy

이 정책은 Amazon에 AWS Glue 데이터를 카탈로그에 게시할 DataZone 권한을 부여합니다. 또한 Amazon에 카탈로그에 있는 AWS Glue 게시 자산에 대한 액세스 DataZone 권한을 부여하거나 액세스 권한을 취소할 수 있는 권한을 부여합니다.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "GlueDataQualityPermissions",
   "Effect": "Allow",
   "Action": [
    "glue:ListDataQualityResults",
    "glue:GetDataQualityResult"
   ],
   "Resource": "arn:aws:glue:*:*:dataQualityRuleset/*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
  },
  {
   "Sid": "GlueTableDatabasePermissions",
   "Effect": "Allow",
   "Action": [
    "glue:CreateTable",
    "glue:DeleteTable",
    "glue:GetDatabases",
    "glue:GetTables"
   ],
   "Resource": [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/*",
    "arn:aws:glue:*:*:table/*"
   ],
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
  },
  {
   "Sid": "LakeformationResourceSharingPermissions",
   "Effect": "Allow",
   "Action": [
    "lakeformation:BatchGrantPermissions",
    "lakeformation:BatchRevokePermissions",
    "lakeformation:CreateLakeFormationOptIn",
```

```
    "lakeformation:DeleteLakeFormationOptIn",
    "lakeformation:GrantPermissions",
    "lakeformation:GetResourceLFTags",
    "lakeformation:ListLakeFormationOptIns",
    "lakeformation:ListPermissions",
    "lakeformation:RegisterResource",
    "lakeformation:RevokePermissions",
    "glue:GetDatabase",
    "glue:GetTable",
    "organizations:DescribeOrganization",
    "ram:GetResourceShareInvitations",
    "ram:ListResources"
   ],
   "Resource": "*"
  },
  {
   "Sid": "CrossAccountRAMResourceSharingPermissions",
   "Effect": "Allow",
   "Action": [
    "glue:DeleteResourcePolicy",
    "glue:PutResourcePolicy"
   ],
   "Resource": [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/*",
    "arn:aws:glue:*:*:table/*"
   ],
   "Condition": {
    "ForAnyValue:StringEquals": {
     "aws:CalledVia": [
      "ram.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "CrossAccountLakeFormationResourceSharingPermissions",
   "Effect": "Allow",
   "Action": [
    "ram:CreateResourceShare"
   ],
   "Resource": "*",
   "Condition": {
    "StringEqualsIfExists": {
```

```
     "ram:RequestedResourceType": [
      "glue:Table",
      "glue:Database",
      "glue:Catalog"
     ]
    },
    "ForAnyValue:StringEquals": {
     "aws:CalledVia": [
      "lakeformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "CrossAccountRAMResourceShareInvitationPermission",
   "Effect": "Allow",
   "Action": [
    "ram:AcceptResourceShareInvitation"
   ],
   "Resource": "arn:aws:ram:*:*:resource-share-invitation/*"
  },
  {
   "Sid": "CrossAccountRAMResourceSharingViaLakeFormationPermissions",
   "Effect": "Allow",
   "Action": [
    "ram:AssociateResourceShare",
    "ram:DeleteResourceShare",
    "ram:DisassociateResourceShare",
    "ram:GetResourceShares",
    "ram:ListResourceSharePermissions",
    "ram:UpdateResourceShare"
   ],
   "Resource": "*",
   "Condition": {
    "StringLike": {
     "ram:ResourceShareName": [
      "LakeFormation*"
     ]
    },
    "ForAnyValue:StringEquals": {
     "aws:CalledVia": [
      "lakeformation.amazonaws.com"
     ]
    }
```

```
    }
   },
   {
    "Sid": "CrossAccountRAMResourceSharingViaLakeFormationHybrid",
    "Effect": "Allow",
    "Action": "ram:AssociateResourceSharePermission",
    "Resource": "*",
    "Condition": {
     "StringLike": {
      "ram:PermissionArn": "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
     },
     "ForAnyValue:StringEquals": {
      "aws:CalledVia": [
       "lakeformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "KMSDecryptPermission",
    "Effect": "Allow",
    "Action": [
     "kms:Decrypt"
    ],
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceTag/datazone:projectId": "proj-all"
     }
    }
   },
   {
    "Sid": "GetRoleForDataZone",
    "Effect": "Allow",
    "Action": [
     "iam:GetRole"
    ],
    "Resource": [
     "arn:aws:iam::*:role/AmazonDataZone*",
     "arn:aws:iam::*:role/service-role/AmazonDataZone*"
    ]
   },
   {
    "Sid": "PassRoleForDataLocationRegistration",
```

```
    "Effect": "Allow",
    "Action": [
     "iam:PassRole"
    ],
    "Resource": [
     "arn:aws:iam::*:role/AmazonDataZone*",
     "arn:aws:iam::*:role/service-role/AmazonDataZone*"
    ],
    "Condition": {
     "StringEquals": {
      "iam:PassedToService": [
       "lakeformation.amazonaws.com"
      ]
     }
    }
   }
  ]
}
```

AWS 관리형 정책: AmazonDataZoneRedshiftManageAccessRolePolicy

이 정책은 Amazon에 Amazon Redshift 데이터를 카탈로그에 게시할 DataZone 권한을 부여합니다. 또한 카탈로그에 있는 Amazon Redshift 또는 Amazon Redshift 서버리스에 게시된 자산에 대한 액세스 DataZone 권한을 부여하거나 액세스 권한을 취소할 수 있는 권한을 아마존에 부여합니다.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "redshiftDataScopeDownPermissions",
   "Effect": "Allow",
   "Action": [
    "redshift-data:BatchExecuteStatement",
    "redshift-data:DescribeTable",
    "redshift-data:ExecuteStatement",
    "redshift-data:ListTables",
    "redshift-data:ListSchemas",
    "redshift-data:ListDatabases"
   ],
   "Resource": [
    "arn:aws:redshift-serverless:*:*:workgroup/*",
```

```
     "arn:aws:redshift:*:*:cluster:*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   },
   {
    "Sid": "listSecretsPermission",
    "Effect": "Allow",
    "Action": "secretsmanager:ListSecrets",
    "Resource": "*"
   },
   {
    "Sid": "getWorkgroupPermission",
    "Effect": "Allow",
    "Action": "redshift-serverless:GetWorkgroup",
    "Resource": [
     "arn:aws:redshift-serverless:*:*:workgroup/*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   },
   {
    "Sid": "getNamespacePermission",
    "Effect": "Allow",
    "Action": "redshift-serverless:GetNamespace",
    "Resource": [
     "arn:aws:redshift-serverless:*:*:namespace/*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   },
   {
    "Sid": "redshiftDataPermissions",
    "Effect": "Allow",
    "Action": [
```

```
    "redshift-data:DescribeStatement",
    "redshift-data:GetStatementResult",
    "redshift:DescribeClusters"
   ],
   "Resource": "*"
  },
  {
   "Sid": "dataSharesPermissions",
   "Effect": "Allow",
   "Action": [
    "redshift:AuthorizeDataShare",
    "redshift:DescribeDataShares"
   ],
   "Resource": [
    "arn:aws:redshift:*:*:datashare:*/datazone*"
   ],
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
  },
  {
   "Sid": "associateDataShareConsumerPermission",
   "Effect": "Allow",
   "Action": "redshift:AssociateDataShareConsumer",
   "Resource": "arn:aws:redshift:*:*:datashare:*/datazone*"
  }
 ]
}
```

AWS 관리형 정책: AmazonDataZoneCrossAccountAdmin

AmazonDataZoneCrossAccountAdmin 정책을 IAM ID에 연결할 수 있습니다.

이 정책을 통해 사용자는 Amazon DataZone 관련 계정을 사용할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Action": [
                "ram:UpdateResourceShare",
                "ram:DeleteResourceShare",
                "ram:AssociateResourceShare",
                "ram:DisassociateResourceShare",
                "ram:GetResourceShares"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "ram:ResourceShareName": [
                        "DataZone*"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "datazone:PutEnvironmentBlueprintConfiguration",
                "datazone:GetEnvironmentBlueprintConfiguration",
                "datazone:DeleteEnvironmentBlueprintConfiguration",
                "datazone:ListEnvironmentBlueprintConfigurations",
                "datazone:ListDomains",
                "datazone:GetDomain",
                "datazone:GetEnvironmentBlueprint",
                "datazone:ListEnvironmentBlueprints",
                "datazone:ListEnvironments",
                "datazone:GetEnvironment",
                "ram:AcceptResourceShareInvitation",
                "ram:RejectResourceShareInvitation",
                "ram:Get*",
                "ram:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 관리형 정책: AmazonDataZoneDomainExecutionRolePolicy

Amazon DataZone `DomainExecutionRole` 서비스 역할의 기본 정책입니다. Amazon은 이 역할을 DataZone 사용하여 Amazon DataZone 도메인의 데이터를 카탈로그, 검색, 관리, 공유 및 분석합니다.

정책을 귀하의 AmazonDataZoneDomainExecutionRolePolicy `AmazonDataZoneDomainExecutionRole` 정책에 첨부할 수 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DomainExecutionRoleStatement",
      "Effect": "Allow",
      "Action": [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:CancelSubscription",
        "datazone:CreateAsset",
        "datazone:CreateAssetRevision",
        "datazone:CreateAssetType",
        "datazone:CreateDataSource",
        "datazone:CreateEnvironment",
        "datazone:CreateEnvironmentBlueprint",
        "datazone:CreateEnvironmentProfile",
        "datazone:CreateFormType",
        "datazone:CreateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateProjectMembership",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset",
        "datazone:DeleteAssetType",
        "datazone:DeleteDataSource",
        "datazone:DeleteEnvironment",
        "datazone:DeleteEnvironmentBlueprint",
        "datazone:DeleteEnvironmentProfile",
        "datazone:DeleteFormType",
        "datazone:DeleteGlossary",
        "datazone:DeleteGlossaryTerm",
```

```
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteProjectMembership",
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:DeleteSubscriptionTarget",
        "datazone:GetAsset",
        "datazone:GetAssetType",
        "datazone:GetDataSource",
        "datazone:GetDataSourceRun",
        "datazone:GetDomain",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentActionLink",
        "datazone:GetEnvironmentBlueprint",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetEnvironmentProfile",
        "datazone:GetFormType",
        "datazone:GetGlossary",
        "datazone:GetGlossaryTerm",
        "datazone:GetGroupProfile",
        "datazone:GetListing",
        "datazone:GetProject",
        "datazone:GetSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:GetSubscriptionGrant",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:GetSubscriptionTarget",
        "datazone:GetUserProfile",
        "datazone:ListAccountEnvironments",
        "datazone:ListAssetRevisions",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSources",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentBlueprintConfigurationSummaries",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListEnvironments",
        "datazone:ListGroupsForUser",
        "datazone:ListNotifications",
        "datazone:ListProjectMemberships",
        "datazone:ListProjects",
        "datazone:ListSubscriptionGrants",
        "datazone:ListSubscriptionRequests",
```

```
        "datazone:ListSubscriptionTargets",
        "datazone:ListSubscriptions",
        "datazone:ListWarehouseMetadata",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RevokeSubscription",
        "datazone:Search",
        "datazone:SearchGroupProfiles",
        "datazone:SearchListings",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:StartDataSourceRun",
        "datazone:UpdateDataSource",
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentBlueprint",
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:UpdateEnvironmentProfile",
        "datazone:UpdateGlossary",
        "datazone:UpdateGlossaryTerm",
        "datazone:UpdateProject",
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:UpdateSubscriptionRequest",
        "datazone:StartMetadataGenerationRun",
        "datazone:GetMetadataGenerationRun",
        "datazone:CancelMetadataGenerationRun",
        "datazone:ListMetadataGenerationRuns"
      ],
      "Resource": "*"
    },
    {
      "Sid": "RAMResourceShareStatement",
      "Effect": "Allow",
      "Action": "ram:GetResourceShareAssociations",
      "Resource": "*"
    }
  ]
}
```

AWS 관리형 정책: AmazonDataZoneSageMakerProvisioning

이 AmazonDataZoneSageMakerProvisioning 정책은 DataZone Amazon과 상호 운용하는 데 필요한 권한을 SageMaker Amazon에 부여합니다.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "CreateSageMakerStudio",
   "Effect": "Allow",
   "Action": [
    "sagemaker:CreateDomain"
   ],
   "Resource": [
    "*"
   ],
   "Condition": {
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    },
    "ForAnyValue:StringEquals": {
     "aws:TagKeys": [
      "AmazonDataZoneEnvironment"
     ]
    },
    "Null": {
     "aws:TagKeys": "false",
     "aws:ResourceTag/AmazonDataZoneEnvironment": "false",
     "aws:RequestTag/AmazonDataZoneEnvironment": "false"
    }
   }
  },
  {
   "Sid": "DeleteSageMakerStudio",
   "Effect": "Allow",
   "Action": [
    "sagemaker:DeleteDomain"
   ],
   "Resource": [
    "*"
   ],
   "Condition": {
    "StringEquals": {
     "aws:CalledViaFirst": [
```

```
      "cloudformation.amazonaws.com"
     ]
    },
    "ForAnyValue:StringLike": {
     "aws:TagKeys": [
      "AmazonDataZoneEnvironment"
     ]
    },
    "Null": {
     "aws:TagKeys": "false",
     "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
    }
   }
  },
  {
   "Sid": "AmazonDataZoneEnvironmentSageMakerDescribePermissions",
   "Effect": "Allow",
   "Action": [
    "sagemaker:DescribeDomain"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "IamPassRolePermissions",
   "Effect": "Allow",
   "Action": [
    "iam:PassRole"
   ],
   "Resource": [
    "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
   ],
   "Condition": {
    "StringEquals": {
     "iam:PassedToService": [
      "glue.amazonaws.com",
      "lakeformation.amazonaws.com",
      "sagemaker.amazonaws.com"
```

```
      ],
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AmazonDataZonePermissionsToCreateEnvironmentRole",
    "Effect": "Allow",
    "Action": [
     "iam:CreateRole",
     "iam:DetachRolePolicy",
     "iam:DeleteRolePolicy",
     "iam:AttachRolePolicy",
     "iam:PutRolePolicy"
    ],
    "Resource": [
     "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ],
      "iam:PermissionsBoundary": "arn:aws:iam::aws:policy/
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary"
     }
    }
   },
   {
    "Sid": "AmazonDataZonePermissionsToManageEnvironmentRole",
    "Effect": "Allow",
    "Action": [
     "iam:GetRole",
     "iam:GetRolePolicy",
     "iam:DeleteRole"
    ],
    "Resource": [
     "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
```

```
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AmazonDataZonePermissionsToCreateSageMakerServiceRole",
   "Effect": "Allow",
   "Action": [
    "iam:CreateServiceLinkedRole"
   ],
   "Resource": [
    "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks"
   ],
   "Condition": {
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AmazonDataZoneEnvironmentParameterValidation",
   "Effect": "Allow",
   "Action": [
    "ec2:DescribeVpcs",
    "ec2:DescribeSubnets",
    "sagemaker:ListDomains"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AmazonDataZoneEnvironmentKMSKeyValidation",
   "Effect": "Allow",
   "Action": [
    "kms:DescribeKey"
   ],
   "Resource": "arn:aws:kms:*:*:key/*",
   "Condition": {
    "Null": {
     "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
    }
```

```
    }
   },
   {
    "Sid": "AmazonDataZoneEnvironmentGluePermissions",
    "Effect": "Allow",
    "Action": [
     "glue:CreateConnection",
     "glue:DeleteConnection"
    ],
    "Resource": [
     "arn:aws:glue:*:*:connection/dz-sm-athena-glue-connection-*",
     "arn:aws:glue:*:*:connection/dz-sm-redshift-cluster-connection-*",
     "arn:aws:glue:*:*:connection/dz-sm-redshift-serverless-connection-*",
     "arn:aws:glue:*:*:catalog"
    ],
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   }
  ]
}
```

AWS 관리형 정책: AmazonDataZoneSageMakerAccess

이 정책은 Amazon에 Amazon SageMaker 자산을 카탈로그에 게시할 DataZone 권한을 부여합니다. 또한 Amazon에 카탈로그에 SageMaker 게시된 자산에 대한 액세스 DataZone 권한을 부여하거나 액세스 권한을 취소할 수 있는 권한을 Amazon에 부여합니다.

이 정책에는 다음을 할 수 있는 권한이 포함되어 있습니다.

- cloudtrail — 트레일에 대한 정보를 검색합니다. CloudTrail
- 클라우드워치 — 현재 경보를 검색합니다. CloudWatch
- 로그 — 로그에 대한 지표 필터를 검색합니다. CloudWatch
- sns — SNS 주제에 대한 구독 목록을 검색합니다.
- config — 구성 레코더, 리소스 및 Config AWS 규칙에 대한 정보를 검색합니다. 또한 서비스 연결 역할이 AWS Config 규칙을 생성 및 삭제하고 규칙에 대한 평가를 실행할 수 있습니다.

- iam — 계정에 대한 자격 증명 보고서를 가져오고 생성합니다.
- 조직 — 조직의 계정 및 OU (조직 구성 단위) 정보를 검색합니다.
- securityhub — Security Hub 서비스, 표준 및 제어가 구성된 방식에 대한 정보를 검색합니다.
- 태그 - 리소스 태그에 대한 정보를 검색합니다.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AmazonSageMakerReadPermission",
   "Effect": "Allow",
   "Action": [
    "sagemaker:DescribeFeatureGroup",
    "sagemaker:ListModelPackages",
    "sagemaker:DescribeModelPackage",
    "sagemaker:DescribeModelPackageGroup",
    "sagemaker:DescribeAlgorithm",
    "sagemaker:ListTags",
    "sagemaker:DescribeDomain",
    "sagemaker:GetModelPackageGroupPolicy",
    "sagemaker:Search"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AmazonSageMakerTaggingPermission",
   "Effect": "Allow",
   "Action": [
    "sagemaker:AddTags",
    "sagemaker:DeleteTags"
   ],
   "Resource": "*",
   "Condition": {
    "ForAnyValue:StringLike": {
     "aws:TagKeys": [
      "sagemaker:shared-with:*"
     ]
    }
   }
  },
```

```
{
 "Sid": "AmazonSageMakerModelPackageGroupPolicyPermission",
 "Effect": "Allow",
 "Action": [
  "sagemaker:PutModelPackageGroupPolicy",
  "sagemaker:DeleteModelPackageGroupPolicy"
 ],
 "Resource": [
  "arn:*:sagemaker:*:*:model-package-group/*"
 ]
},
{
 "Sid": "AmazonSageMakerRAMPermission",
 "Effect": "Allow",
 "Action": [
  "ram:GetResourceShares",
  "ram:GetResourceShareInvitations",
  "ram:GetResourceShareAssociations"
 ],
 "Resource": "*"
},
{
 "Sid": "AmazonSageMakerRAMResourcePolicyPermission",
 "Effect": "Allow",
 "Action": [
  "sagemaker:PutResourcePolicy",
  "sagemaker:GetResourcePolicy",
  "sagemaker:DeleteResourcePolicy"
 ],
 "Resource": [
  "arn:*:sagemaker:*:*:feature-group/*"
 ]
},
{
 "Sid": "AmazonSageMakerRAMTagResourceSharePermission",
 "Effect": "Allow",
 "Action": [
  "ram:TagResource"
 ],
 "Resource": "arn:*:ram:*:*:resource-share/*",
 "Condition": {
  "Null": {
   "aws:RequestTag/AwsDataZoneDomainId": "false"
  }
```

```
    }
   },
   {
    "Sid": "AmazonSageMakerRAMDeleteResourceSharePermission",
    "Effect": "Allow",
    "Action": [
     "ram:DeleteResourceShare"
    ],
    "Resource": "arn:*:ram:*:*:resource-share/*",
    "Condition": {
     "Null": {
      "aws:ResourceTag/AwsDataZoneDomainId": "false"
     }
    }
   },
   {
    "Sid": "AmazonSageMakerRAMCreateResourceSharePermission",
    "Effect": "Allow",
    "Action": [
     "ram:CreateResourceShare"
    ],
    "Resource": "*",
    "Condition": {
     "StringLikeIfExists": {
      "ram:RequestedResourceType": [
       "sagemaker:*"
      ]
     },
     "Null": {
      "aws:RequestTag/AwsDataZoneDomainId": "false"
     }
    }
   },
   {
    "Sid": "AmazonSageMakerS3BucketPolicyPermission",
    "Effect": "Allow",
    "Action": [
     "s3:DeleteBucketPolicy",
     "s3:PutBucketPolicy",
     "s3:GetBucketPolicy"
    ],
    "Resource": [
     "arn:aws:s3:::sagemaker-datazone*",
     "arn:aws:s3:::SageMaker-DataZone*",
```

```
    "arn:aws:s3:::datazone-sagemaker*",
    "arn:aws:s3:::DataZone-SageMaker*",
    "arn:aws:s3:::amazon-datazone*"
   ]
  },
  {
   "Sid": "AmazonSageMakerS3Permission",
   "Effect": "Allow",
   "Action": [
    "s3:GetObject",
    "s3:ListBucket"
   ],
   "Resource": [
    "arn:aws:s3:::sagemaker-datazone*",
    "arn:aws:s3:::SageMaker-DataZone*",
    "arn:aws:s3:::datazone-sagemaker*",
    "arn:aws:s3:::DataZone-SageMaker*",
    "arn:aws:s3:::amazon-datazone*"
   ]
  },
  {
   "Sid": "AmazonSageMakerECRPermission",
   "Effect": "Allow",
   "Action": [
    "ecr:GetRepositoryPolicy",
    "ecr:SetRepositoryPolicy",
    "ecr:DeleteRepositoryPolicy"
   ],
   "Resource": "*",
   "Condition": {
    "Null": {
     "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
    }
   }
  },
  {
   "Sid": "AmazonSageMakerKMSReadPermission",
   "Effect": "Allow",
   "Action": [
    "kms:DescribeKey"
   ],
   "Resource": "*",
   "Condition": {
    "ForAnyValue:StringEquals": {
```

```
      "aws:TagKeys": [
       "AmazonDataZoneEnvironment"
      ]
     }
    }
   },
   {
    "Sid": "AmazonSageMakerKMSGrantPermission",
    "Effect": "Allow",
    "Action": [
     "kms:CreateGrant"
    ],
    "Resource": "*",
    "Condition": {
     "ForAnyValue:StringEquals": {
      "aws:TagKeys": [
       "AmazonDataZoneEnvironment"
      ]
     },
     "ForAllValues:StringEquals": {
      "kms:GrantOperations": [
       "Decrypt"
      ]
     }
    }
   }
  ]
}
```

AWS 관리형 정책: AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary

> **Note**
>
> 이 정책은 권한 경계입니다. 권한 경계는 ID 기반 정책이 IAM 개체에 부여할 수 있는 최대 권한을 설정합니다. Amazon DataZone 권한 경계 정책을 직접 사용하고 첨부해서는 안 됩니다. Amazon DataZone 권한 경계 정책은 Amazon DataZone 관리 역할에만 연결해야 합니다. 권한 경계에 대한 자세한 내용은 IAM 사용 설명서의 IAM 엔티티의 권한 경계를 참조하십시오.

Amazon DataZone 데이터 포털을 통해 Amazon SageMaker 환경을 생성하면 Amazon은 환경 생성 중에 생성되는 IAM 역할에 이 권한 경계를 DataZone 적용합니다. 권한 경계는 Amazon이 DataZone 생성하는 역할 및 사용자가 추가하는 모든 역할의 범위를 제한합니다.

DataZone Amazon은 AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary 관리형 정책을 사용하여 연결된 프로비저닝된 IAM 보안 주체를 제한합니다. 보안 주체는 Amazon이 대화형 엔터프라이즈 사용자 또는 분석 서비스 (AWS SageMaker예:) 를 대신하여 맡을 DataZone 수 있는 사용자 역할의 형태를 취한 다음 Amazon S3 또는 Amazon Redshift에서 읽고 쓰거나 Glue 크롤러를 실행하는 등의 작업을 수행할 수 있습니다. AWS

이 AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary 정책은 Amazon, AWS Glue SageMaker, Amazon DataZone S3, AWS Lake Formation, Amazon Redshift, Amazon Athena와 같은 서비스에 Amazon에 대한 읽기 및 쓰기 액세스 권한을 부여합니다. 또한 이 정책은 네트워크 인터페이스, Amazon ECR 리포지토리, KMS 키 등 이러한 서비스를 사용하는 데 필요한 일부 인프라 리소스에 읽기 및 AWS 쓰기 권한을 부여합니다. 또한 Amazon SageMaker Canvas와 같은 아마존 SageMaker 애플리케이션에 대한 액세스 권한도 제공합니다.

Amazon은 AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary 관리형 정책을 모든 Amazon DataZone 환경 역할 (소유자 및 기여자) 에 대한 권한 경계로 DataZone 적용합니다. 이 권한 경계는 환경에 필요한 리소스 및 작업에 대한 액세스만 허용하도록 이러한 역할을 제한합니다.

```
       {
"Version": "2012-10-17",
"Statement": [
 {
  "Sid": "AllowAllNonAdminSageMakerActions",
  "Effect": "Allow",
  "Action": [
   "sagemaker:*",
   "sagemaker-geospatial:*"
  ],
  "NotResource": [
   "arn:aws:sagemaker:*:*:domain/*",
   "arn:aws:sagemaker:*:*:user-profile/*",
   "arn:aws:sagemaker:*:*:app/*",
   "arn:aws:sagemaker:*:*:space/*",
   "arn:aws:sagemaker:*:*:flow-definition/*"
  ]
 },
 {
```

```
    "Sid": "AllowSageMakerProfileManagement",
    "Effect": "Allow",
    "Action": [
     "sagemaker:CreateUserProfile",
     "sagemaker:DescribeUserProfile",
     "sagemaker:UpdateUserProfile",
     "sagemaker:CreatePresignedDomainUrl"
    ],
    "Resource": "arn:aws:sagemaker:*:*:*/*"
   },
   {
    "Sid": "AllowLakeFormation",
    "Effect": "Allow",
    "Action": [
     "lakeformation:GetDataAccess"
    ],
    "Resource": "*"
   },
   {
    "Sid": "AllowAddTagsForAppAndSpace",
    "Effect": "Allow",
    "Action": [
     "sagemaker:AddTags"
    ],
    "Resource": [
     "arn:aws:sagemaker:*:*:app/*",
     "arn:aws:sagemaker:*:*:space/*"
    ],
    "Condition": {
     "StringEquals": {
      "sagemaker:TaggingAction": [
       "CreateApp",
       "CreateSpace"
      ]
     }
    }
   },
   {
    "Sid": "AllowStudioActions",
    "Effect": "Allow",
    "Action": [
     "sagemaker:CreatePresignedDomainUrl",
     "sagemaker:DescribeApp",
     "sagemaker:DescribeDomain",
```

```
    "sagemaker:DescribeSpace",
    "sagemaker:DescribeUserProfile",
    "sagemaker:ListApps",
    "sagemaker:ListDomains",
    "sagemaker:ListSpaces",
    "sagemaker:ListUserProfiles"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowAppActionsForUserProfile",
   "Effect": "Allow",
   "Action": [
    "sagemaker:CreateApp",
    "sagemaker:DeleteApp"
   ],
   "Resource": "arn:aws:sagemaker:*:*:app/*/*/*/*",
   "Condition": {
    "Null": {
     "sagemaker:OwnerUserProfileArn": "true"
    }
   }
  },
  {
   "Sid": "AllowAppActionsForSharedSpaces",
   "Effect": "Allow",
   "Action": [
    "sagemaker:CreateApp",
    "sagemaker:DeleteApp"
   ],
   "Resource": "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
   "Condition": {
    "StringEquals": {
     "sagemaker:SpaceSharingType": [
      "Shared"
     ]
    }
   }
  },
  {
   "Sid": "AllowMutatingActionsOnSharedSpacesWithoutOwner",
   "Effect": "Allow",
   "Action": [
    "sagemaker:CreateSpace",
```

```
    "sagemaker:DeleteSpace",
    "sagemaker:UpdateSpace"
   ],
   "Resource": "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
   "Condition": {
    "Null": {
     "sagemaker:OwnerUserProfileArn": "true"
    }
   }
  },
  {
   "Sid": "RestrictMutatingActionsOnSpacesToOwnerUserProfile",
   "Effect": "Allow",
   "Action": [
    "sagemaker:CreateSpace",
    "sagemaker:DeleteSpace",
    "sagemaker:UpdateSpace"
   ],
   "Resource": "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
   "Condition": {
    "ArnLike": {
     "sagemaker:OwnerUserProfileArn": "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
    },
    "StringEquals": {
     "sagemaker:SpaceSharingType": [
      "Private",
      "Shared"
     ]
    }
   }
  },
  {
   "Sid": "RestrictMutatingActionsOnPrivateSpaceAppsToOwnerUserProfile",
   "Effect": "Allow",
   "Action": [
    "sagemaker:CreateApp",
    "sagemaker:DeleteApp"
   ],
   "Resource": "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
   "Condition": {
    "ArnLike": {
     "sagemaker:OwnerUserProfileArn": "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
```

```
    },
    "StringEquals": {
     "sagemaker:SpaceSharingType": [
      "Private"
     ]
    }
   }
  },
  {
   "Sid": "AllowFlowDefinitionActions",
   "Effect": "Allow",
   "Action": "sagemaker:*",
   "Resource": [
    "arn:aws:sagemaker:*:*:flow-definition/*"
   ],
   "Condition": {
    "StringEqualsIfExists": {
     "sagemaker:WorkteamType": [
      "private-crowd",
      "vendor-crowd"
     ]
    }
   }
  },
  {
   "Sid": "AllowAWSServiceActions",
   "Effect": "Allow",
   "Action": [
    "sqlworkbench:*",
    "datazone:*",
    "application-autoscaling:DeleteScalingPolicy",
    "application-autoscaling:DeleteScheduledAction",
    "application-autoscaling:DeregisterScalableTarget",
    "application-autoscaling:DescribeScalableTargets",
    "application-autoscaling:DescribeScalingActivities",
    "application-autoscaling:DescribeScalingPolicies",
    "application-autoscaling:DescribeScheduledActions",
    "application-autoscaling:PutScalingPolicy",
    "application-autoscaling:PutScheduledAction",
    "application-autoscaling:RegisterScalableTarget",
    "aws-marketplace:ViewSubscriptions",
    "cloudformation:GetTemplateSummary",
    "cloudwatch:DeleteAlarms",
    "cloudwatch:DescribeAlarms",
```

```
    "cloudwatch:GetMetricData",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "cloudwatch:PutMetricAlarm",
    "cloudwatch:PutMetricData",
    "codecommit:BatchGetRepositories",
    "codecommit:CreateRepository",
    "codecommit:GetRepository",
    "codecommit:List*",
    "ec2:CreateNetworkInterface",
    "ec2:CreateNetworkInterfacePermission",
    "ec2:DeleteNetworkInterface",
    "ec2:DeleteNetworkInterfacePermission",
    "ec2:DescribeDhcpOptions",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcEndpointServices",
    "ec2:DescribeVpcs",
    "ecr:BatchCheckLayerAvailability",
    "ecr:BatchGetImage",
    "ecr:Describe*",
    "ecr:GetAuthorizationToken",
    "ecr:GetDownloadUrlForLayer",
    "ecr:StartImageScan",
    "elastic-inference:Connect",
    "elasticfilesystem:DescribeFileSystems",
    "elasticfilesystem:DescribeMountTargets",
    "fsx:DescribeFileSystems",
    "groundtruthlabeling:*",
    "iam:GetRole",
    "iam:ListRoles",
    "kms:DescribeKey",
    "kms:ListAliases",
    "lambda:ListFunctions",
    "logs:CreateLogDelivery",
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:DeleteLogDelivery",
    "logs:DescribeLogGroups",
    "logs:DescribeLogStreams",
    "logs:GetLogDelivery",
```

```
    "logs:GetLogEvents",
    "logs:ListLogDeliveries",
    "logs:PutLogEvents",
    "logs:UpdateLogDelivery",
    "redshift-data:BatchExecuteStatement",
    "redshift-data:CancelStatement",
    "redshift-data:DescribeStatement",
    "redshift-data:DescribeTable",
    "redshift-data:ExecuteStatement",
    "redshift-data:GetStatementResult",
    "redshift-data:ListSchemas",
    "redshift-data:ListTables",
    "redshift-serverless:GetCredentials",
    "redshift-serverless:GetNamespace",
    "redshift-serverless:GetWorkgroup",
    "redshift-serverless:ListNamespaces",
    "redshift-serverless:ListWorkgroups",
    "secretsmanager:ListSecrets",
    "servicecatalog:Describe*",
    "servicecatalog:List*",
    "servicecatalog:ScanProvisionedProducts",
    "servicecatalog:SearchProducts",
    "servicecatalog:SearchProvisionedProducts",
    "sns:ListTopics",
    "tag:GetResources"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowRAMInvitation",
   "Effect": "Allow",
   "Action": "ram:AcceptResourceShareInvitation",
   "Resource": "*",
   "Condition": {
    "StringLike": {
     "ram:ResourceShareName": "dzd_*"
    }
   }
  },
  {
   "Sid": "AllowECRActions",
   "Effect": "Allow",
   "Action": [
    "ecr:SetRepositoryPolicy",
```

```
    "ecr:CompleteLayerUpload",
    "ecr:CreateRepository",
    "ecr:BatchDeleteImage",
    "ecr:UploadLayerPart",
    "ecr:DeleteRepositoryPolicy",
    "ecr:InitiateLayerUpload",
    "ecr:DeleteRepository",
    "ecr:PutImage",
    "ecr:TagResource",
    "ecr:UntagResource"
   ],
   "Resource": [
    "arn:aws:ecr:*:*:repository/sagemaker*",
    "arn:aws:ecr:*:*:repository/datazone*"
   ]
  },
  {
   "Sid": "AllowCodeCommitActions",
   "Effect": "Allow",
   "Action": [
    "codecommit:GitPull",
    "codecommit:GitPush"
   ],
   "Resource": [
    "arn:aws:codecommit:*:*:*sagemaker*",
    "arn:aws:codecommit:*:*:*SageMaker*",
    "arn:aws:codecommit:*:*:*Sagemaker*"
   ]
  },
  {
   "Sid": "AllowCodeBuildActions",
   "Action": [
    "codebuild:BatchGetBuilds",
    "codebuild:StartBuild"
   ],
   "Resource": [
    "arn:aws:codebuild:*:*:project/sagemaker*",
    "arn:aws:codebuild:*:*:build/*"
   ],
   "Effect": "Allow"
  },
  {
   "Sid": "AllowStepFunctionsActions",
   "Action": [
```

```
    "states:DescribeExecution",
    "states:GetExecutionHistory",
    "states:StartExecution",
    "states:StopExecution",
    "states:UpdateStateMachine"
   ],
   "Resource": [
    "arn:aws:states:*:*:statemachine:*sagemaker*",
    "arn:aws:states:*:*:execution:*sagemaker*:*"
   ],
   "Effect": "Allow"
  },
  {
   "Sid": "AllowSecretManagerActions",
   "Effect": "Allow",
   "Action": [
    "secretsmanager:DescribeSecret",
    "secretsmanager:GetSecretValue",
    "secretsmanager:CreateSecret",
    "secretsmanager:PutResourcePolicy"
   ],
   "Resource": [
    "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
   ]
  },
  {
   "Sid": "AllowServiceCatalogProvisionProduct",
   "Effect": "Allow",
   "Action": [
    "servicecatalog:ProvisionProduct"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowServiceCatalogTerminateUpdateProvisionProduct",
   "Effect": "Allow",
   "Action": [
    "servicecatalog:TerminateProvisionedProduct",
    "servicecatalog:UpdateProvisionedProduct"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "servicecatalog:userLevel": "self"
```

```
    }
   }
  },
  {
   "Sid": "AllowS3ObjectActions",
   "Effect": "Allow",
   "Action": [
    "s3:AbortMultipartUpload",
    "s3:DeleteObject",
    "s3:DeleteObjectVersion",
    "s3:GetObject",
    "s3:PutObject",
    "s3:PutObjectRetention",
    "s3:ReplicateObject",
    "s3:RestoreObject",
    "s3:GetBucketAcl",
    "s3:PutObjectAcl"
   ],
   "Resource": [
    "arn:aws:s3:::SageMaker-DataZone*",
    "arn:aws:s3:::DataZone-SageMaker*",
    "arn:aws:s3:::Sagemaker-DataZone*",
    "arn:aws:s3:::DataZone-Sagemaker*",
    "arn:aws:s3:::sagemaker-datazone*",
    "arn:aws:s3:::datazone-sagemaker*",
    "arn:aws:s3:::amazon-datazone*"
   ]
  },
  {
   "Sid": "AllowS3GetObjectWithSageMakerExistingObjectTag",
   "Effect": "Allow",
   "Action": [
    "s3:GetObject"
   ],
   "Resource": [
    "arn:aws:s3:::*"
   ],
   "Condition": {
    "StringEqualsIgnoreCase": {
     "s3:ExistingObjectTag/SageMaker": "true"
    }
   }
  },
  {
```

```
    "Sid": "AllowS3GetObjectWithServiceCatalogProvisioningExistingObjectTag",
    "Effect": "Allow",
    "Action": [
     "s3:GetObject"
    ],
    "Resource": [
     "arn:aws:s3:::*"
    ],
    "Condition": {
     "StringEquals": {
      "s3:ExistingObjectTag/servicecatalog:provisioning": "true"
     }
    }
   },
   {
    "Sid": "AllowS3BucketActions",
    "Effect": "Allow",
    "Action": [
     "s3:GetBucketLocation",
     "s3:ListBucket",
     "s3:ListAllMyBuckets",
     "s3:GetBucketCors",
     "s3:PutBucketCors"
    ],
    "Resource": [
     "arn:aws:s3:::SageMaker-DataZone*",
     "arn:aws:s3:::DataZone-SageMaker*",
     "arn:aws:s3:::Sagemaker-DataZone*",
     "arn:aws:s3:::DataZone-Sagemaker*",
     "arn:aws:s3:::sagemaker-datazone*",
     "arn:aws:s3:::datazone-sagemaker*",
     "arn:aws:s3:::amazon-datazone*"
    ]
   },
   {
    "Sid": "ReadSageMakerJumpstartArtifacts",
    "Effect": "Allow",
    "Action": "s3:GetObject",
    "Resource": [
     "arn:aws:s3:::jumpstart-cache-prod-us-west-2/*",
     "arn:aws:s3:::jumpstart-cache-prod-us-east-1/*",
     "arn:aws:s3:::jumpstart-cache-prod-us-east-2/*",
     "arn:aws:s3:::jumpstart-cache-prod-eu-west-1/*",
     "arn:aws:s3:::jumpstart-cache-prod-eu-central-1/*",
```

```
    "arn:aws:s3:::jumpstart-cache-prod-ap-south-1/*",
    "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-2/*",
    "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-1/*",
    "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-1/*",
    "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-2/*"
   ]
  },
  {
   "Sid": "AllowLambdaInvokeFunction",
   "Effect": "Allow",
   "Action": [
    "lambda:InvokeFunction"
   ],
   "Resource": [
    "arn:aws:lambda:*:*:function:*SageMaker*",
    "arn:aws:lambda:*:*:function:*sagemaker*",
    "arn:aws:lambda:*:*:function:*Sagemaker*",
    "arn:aws:lambda:*:*:function:*LabelingFunction*"
   ]
  },
  {
   "Sid": "AllowCreateServiceLinkedRoleForSageMakerApplicationAutoscaling",
   "Action": "iam:CreateServiceLinkedRole",
   "Effect": "Allow",
   "Resource": "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
   "Condition": {
    "StringLike": {
     "iam:AWSServiceName": "sagemaker.application-autoscaling.amazonaws.com"
    }
   }
  },
  {
   "Sid": "AllowSNSActions",
   "Effect": "Allow",
   "Action": [
    "sns:Subscribe",
    "sns:CreateTopic",
    "sns:Publish"
   ],
   "Resource": [
    "arn:aws:sns:*:*:*SageMaker*",
    "arn:aws:sns:*:*:*Sagemaker*",
    "arn:aws:sns:*:*:*sagemaker*"
```

```
    ]
   },
   {
    "Sid": "AllowPassRoleForSageMakerRoles",
    "Effect": "Allow",
    "Action": [
     "iam:PassRole"
    ],
    "Resource": [
     "arn:aws:iam::*:role/sm-provisioning/datazone_usr_sagemaker_execution_role_*"
    ],
    "Condition": {
     "StringEquals": {
      "iam:PassedToService": [
       "glue.amazonaws.com",
       "bedrock.amazonaws.com",
       "states.amazonaws.com",
       "lakeformation.amazonaws.com",
       "events.amazonaws.com",
       "sagemaker.amazonaws.com",
       "forecast.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "CrossAccountKmsOperations",
    "Effect": "Allow",
    "Action": [
     "kms:DescribeKey",
     "kms:Decrypt",
     "kms:ListKeys"
    ],
    "Resource": "*",
    "Condition": {
     "StringNotEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   },
   {
    "Sid": "KmsOperationsWithResourceTag",
    "Effect": "Allow",
    "Action": [
```

```
    "kms:DescribeKey",
    "kms:Decrypt",
    "kms:ListKeys",
    "kms:Encrypt",
    "kms:GenerateDataKey",
    "kms:RetireGrant"
   ],
   "Resource": "*",
   "Condition": {
    "Null": {
     "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
    }
   }
  },
  {
   "Sid": "AllowAthenaActions",
   "Effect": "Allow",
   "Action": [
    "athena:BatchGetNamedQuery",
    "athena:BatchGetPreparedStatement",
    "athena:BatchGetQueryExecution",
    "athena:CreateNamedQuery",
    "athena:CreateNotebook",
    "athena:CreatePreparedStatement",
    "athena:CreatePresignedNotebookUrl",
    "athena:DeleteNamedQuery",
    "athena:DeleteNotebook",
    "athena:DeletePreparedStatement",
    "athena:ExportNotebook",
    "athena:GetDatabase",
    "athena:GetDataCatalog",
    "athena:GetNamedQuery",
    "athena:GetPreparedStatement",
    "athena:GetQueryExecution",
    "athena:GetQueryResults",
    "athena:GetQueryResultsStream",
    "athena:GetQueryRuntimeStatistics",
    "athena:GetTableMetadata",
    "athena:GetWorkGroup",
    "athena:ImportNotebook",
    "athena:ListDatabases",
    "athena:ListDataCatalogs",
    "athena:ListEngineVersions",
    "athena:ListNamedQueries",
```

```
    "athena:ListPreparedStatements",
    "athena:ListQueryExecutions",
    "athena:ListTableMetadata",
    "athena:ListTagsForResource",
    "athena:ListWorkGroups",
    "athena:StartCalculationExecution",
    "athena:StartQueryExecution",
    "athena:StartSession",
    "athena:StopCalculationExecution",
    "athena:StopQueryExecution",
    "athena:TerminateSession",
    "athena:UpdateNamedQuery",
    "athena:UpdateNotebook",
    "athena:UpdateNotebookMetadata",
    "athena:UpdatePreparedStatement"
   ],
   "Resource": [
    "*"
   ]
  },
  {
   "Sid": "AllowGlueCreateDatabase",
   "Effect": "Allow",
   "Action": [
    "glue:CreateDatabase"
   ],
   "Resource": [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/default"
   ]
  },
  {
   "Sid": "AllowRedshiftGetClusterCredentials",
   "Effect": "Allow",
   "Action": [
    "redshift:GetClusterCredentials"
   ],
   "Resource": [
    "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
    "arn:aws:redshift:*:*:dbname:*"
   ]
  },
  {
   "Sid": "AllowListTags",
```

```
    "Effect": "Allow",
    "Action": [
     "sagemaker:ListTags"
    ],
    "Resource": [
     "arn:aws:sagemaker:*:*:user-profile/*",
     "arn:aws:sagemaker:*:*:domain/*"
    ]
   },
   {
    "Sid": "AllowCloudformationListStackResources",
    "Effect": "Allow",
    "Action": [
     "cloudformation:ListStackResources"
    ],
    "Resource": "arn:aws:cloudformation:*:*:stack/SC-*"
   },
   {
    "Sid": "AllowGlueActions",
    "Effect": "Allow",
    "Action": [
     "glue:GetColumnStatisticsForPartition",
     "glue:GetColumnStatisticsForTable",
     "glue:ListJobs",
     "glue:CreateSession",
     "glue:RunStatement",
     "glue:BatchCreatePartition",
     "glue:CreatePartitionIndex",
     "glue:CreateTable",
     "glue:BatchGetWorkflows",
     "glue:BatchUpdatePartition",
     "glue:BatchDeletePartition",
     "glue:GetPartition",
     "glue:GetPartitions",
     "glue:UpdateTable",
     "glue:DeleteTableVersion",
     "glue:DeleteTable",
     "glue:DeleteColumnStatisticsForPartition",
     "glue:DeleteColumnStatisticsForTable",
     "glue:DeletePartitionIndex",
     "glue:UpdateColumnStatisticsForPartition",
     "glue:UpdateColumnStatisticsForTable",
     "glue:BatchDeleteTableVersion",
     "glue:BatchDeleteTable",
```

```
    "glue:CreatePartition",
    "glue:DeletePartition",
    "glue:UpdatePartition",
    "glue:CreateBlueprint",
    "glue:CreateJob",
    "glue:CreateConnection",
    "glue:CreateCrawler",
    "glue:CreateDataQualityRuleset",
    "glue:CreateWorkflow",
    "glue:GetDatabases",
    "glue:GetTables",
    "glue:GetTable",
    "glue:SearchTables",
    "glue:NotifyEvent",
    "glue:ListSchemas",
    "glue:BatchGetJobs",
    "glue:GetConnection",
    "glue:GetDatabase"
   ],
   "Resource": [
    "*"
   ]
  },
  {
   "Sid": "AllowGlueActionsWithEnvironmentTag",
   "Effect": "Allow",
   "Action": [
    "glue:SearchTables",
    "glue:NotifyEvent",
    "glue:StartBlueprintRun",
    "glue:PutWorkflowRunProperties",
    "glue:StopCrawler",
    "glue:DeleteJob",
    "glue:DeleteWorkflow",
    "glue:UpdateCrawler",
    "glue:DeleteBlueprint",
    "glue:UpdateWorkflow",
    "glue:StartCrawler",
    "glue:ResetJobBookmark",
    "glue:UpdateJob",
    "glue:StartWorkflowRun",
    "glue:StopCrawlerSchedule",
    "glue:ResumeWorkflowRun",
    "glue:ListSchemas",
```

```
    "glue:DeleteCrawler",
    "glue:UpdateBlueprint",
    "glue:BatchStopJobRun",
    "glue:StopWorkflowRun",
    "glue:BatchGetJobs",
    "glue:BatchGetWorkflows",
    "glue:UpdateCrawlerSchedule",
    "glue:DeleteConnection",
    "glue:UpdateConnection",
    "glue:GetConnection",
    "glue:GetDatabase",
    "glue:GetTable",
    "glue:GetPartition",
    "glue:GetPartitions",
    "glue:BatchDeleteConnection",
    "glue:StartCrawlerSchedule",
    "glue:StartJobRun",
    "glue:CreateWorkflow",
    "glue:*DataQuality*"
   ],
   "Resource": "*",
   "Condition": {
    "Null": {
     "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
    }
   }
  },
  {
   "Sid": "AllowGlueDefaultAccess",
   "Effect": "Allow",
   "Action": [
    "glue:BatchGet*",
    "glue:Get*",
    "glue:SearchTables",
    "glue:List*",
    "glue:RunStatement"
   ],
   "Resource": [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/default",
    "arn:aws:glue:*:*:connection/dz-sm-*",
    "arn:aws:glue:*:*:session/*"
   ]
  },
```

```
{
 "Sid": "AllowRedshiftClusterActions",
 "Effect": "Allow",
 "Action": [
  "redshift:GetClusterCredentialsWithIAM",
  "redshift:DescribeClusters"
 ],
 "Resource": [
  "arn:aws:redshift:*:*:cluster:*",
  "arn:aws:redshift:*:*:dbname:*"
 ]
},
{
 "Sid": "AllowCreateClusterUser",
 "Effect": "Allow",
 "Action": [
  "redshift:CreateClusterUser"
 ],
 "Resource": [
  "arn:aws:redshift:*:*:dbuser:*"
 ]
},
{
 "Sid": "AllowCreateSecretActions",
 "Effect": "Allow",
 "Action": [
  "secretsmanager:CreateSecret",
  "secretsmanager:TagResource"
 ],
 "Resource": "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
 "Condition": {
  "StringLike": {
   "aws:ResourceTag/AmazonDataZoneDomain": "dzd_*",
   "aws:RequestTag/AmazonDataZoneDomain": "dzd_*"
  },
  "Null": {
   "aws:TagKeys": "false",
   "aws:ResourceTag/AmazonDataZoneProject": "false",
   "aws:ResourceTag/AmazonDataZoneDomain": "false",
   "aws:RequestTag/AmazonDataZoneDomain": "false",
   "aws:RequestTag/AmazonDataZoneProject": "false"
  },
  "ForAllValues:StringEquals": {
   "aws:TagKeys": [
```

```
      "AmazonDataZoneDomain",
      "AmazonDataZoneProject"
     ]
    }
   }
  },
  {
   "Sid": "ForecastOperations",
   "Effect": "Allow",
   "Action": [
    "forecast:CreateExplainabilityExport",
    "forecast:CreateExplainability",
    "forecast:CreateForecastEndpoint",
    "forecast:CreateAutoPredictor",
    "forecast:CreateDatasetImportJob",
    "forecast:CreateDatasetGroup",
    "forecast:CreateDataset",
    "forecast:CreateForecast",
    "forecast:CreateForecastExportJob",
    "forecast:CreatePredictorBacktestExportJob",
    "forecast:CreatePredictor",
    "forecast:DescribeExplainabilityExport",
    "forecast:DescribeExplainability",
    "forecast:DescribeAutoPredictor",
    "forecast:DescribeForecastEndpoint",
    "forecast:DescribeDatasetImportJob",
    "forecast:DescribeDataset",
    "forecast:DescribeForecast",
    "forecast:DescribeForecastExportJob",
    "forecast:DescribePredictorBacktestExportJob",
    "forecast:GetAccuracyMetrics",
    "forecast:InvokeForecastEndpoint",
    "forecast:GetRecentForecastContext",
    "forecast:DescribePredictor",
    "forecast:TagResource",
    "forecast:DeleteResourceTree"
   ],
   "Resource": [
    "arn:aws:forecast:*:*:*Canvas*"
   ]
  },
  {
   "Sid": "RDSOperation",
   "Effect": "Allow",
```

```
    "Action": "rds:DescribeDBInstances",
    "Resource": "*"
   },
   {
    "Sid": "AllowEventBridgeRule",
    "Effect": "Allow",
    "Action": [
     "events:PutRule"
    ],
    "Resource": "arn:aws:events:*:*:rule/*",
    "Condition": {
     "StringEquals": {
      "aws:RequestTag/sagemaker:is-canvas-data-prep-job": "true"
     }
    }
   },
   {
    "Sid": "EventBridgeOperations",
    "Effect": "Allow",
    "Action": [
     "events:DescribeRule",
     "events:PutTargets"
    ],
    "Resource": "arn:aws:events:*:*:rule/*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceTag/sagemaker:is-canvas-data-prep-job": "true"
     }
    }
   },
   {
    "Sid": "EventBridgeTagBasedOperations",
    "Effect": "Allow",
    "Action": [
     "events:TagResource"
    ],
    "Resource": "arn:aws:events:*:*:rule/*",
    "Condition": {
     "StringEquals": {
      "aws:RequestTag/sagemaker:is-canvas-data-prep-job": "true",
      "aws:ResourceTag/sagemaker:is-canvas-data-prep-job": "true"
     }
    }
   },
```

```
{
 "Sid": "EventBridgeListTagOperation",
 "Effect": "Allow",
 "Action": "events:ListTagsForResource",
 "Resource": "*"
},
{
 "Sid": "AllowEMR",
 "Effect": "Allow",
 "Action": [
  "elasticmapreduce:DescribeCluster",
  "elasticmapreduce:ListInstanceGroups",
  "elasticmapreduce:ListClusters"
 ],
 "Resource": "*"
},
{
 "Sid": "AllowSSOAction",
 "Effect": "Allow",
 "Action": [
  "sso:CreateApplicationAssignment",
  "sso:AssociateProfile"
 ],
 "Resource": "*"
},
{
 "Sid": "DenyNotAction",
 "Effect": "Deny",
 "NotAction": [
  "sagemaker:*",
  "sagemaker-geospatial:*",
  "sqlworkbench:*",
  "datazone:*",
  "forecast:*",
  "application-autoscaling:DeleteScalingPolicy",
  "application-autoscaling:DeleteScheduledAction",
  "application-autoscaling:DeregisterScalableTarget",
  "application-autoscaling:DescribeScalableTargets",
  "application-autoscaling:DescribeScalingActivities",
  "application-autoscaling:DescribeScalingPolicies",
  "application-autoscaling:DescribeScheduledActions",
  "application-autoscaling:PutScalingPolicy",
  "application-autoscaling:PutScheduledAction",
  "application-autoscaling:RegisterScalableTarget",
```

```
    "athena:BatchGetNamedQuery",
    "athena:BatchGetPreparedStatement",
    "athena:BatchGetQueryExecution",
    "athena:CreateNamedQuery",
    "athena:CreateNotebook",
    "athena:CreatePreparedStatement",
    "athena:CreatePresignedNotebookUrl",
    "athena:DeleteNamedQuery",
    "athena:DeleteNotebook",
    "athena:DeletePreparedStatement",
    "athena:ExportNotebook",
    "athena:GetDatabase",
    "athena:GetDataCatalog",
    "athena:GetNamedQuery",
    "athena:GetPreparedStatement",
    "athena:GetQueryExecution",
    "athena:GetQueryResults",
    "athena:GetQueryResultsStream",
    "athena:GetQueryRuntimeStatistics",
    "athena:GetTableMetadata",
    "athena:GetWorkGroup",
    "athena:ImportNotebook",
    "athena:ListDatabases",
    "athena:ListDataCatalogs",
    "athena:ListEngineVersions",
    "athena:ListNamedQueries",
    "athena:ListPreparedStatements",
    "athena:ListQueryExecutions",
    "athena:ListTableMetadata",
    "athena:ListTagsForResource",
    "athena:ListWorkGroups",
    "athena:StartCalculationExecution",
    "athena:StartQueryExecution",
    "athena:StartSession",
    "athena:StopCalculationExecution",
    "athena:StopQueryExecution",
    "athena:TerminateSession",
    "athena:UpdateNamedQuery",
    "athena:UpdateNotebook",
    "athena:UpdateNotebookMetadata",
    "athena:UpdatePreparedStatement",
    "aws-marketplace:ViewSubscriptions",
    "cloudformation:GetTemplateSummary",
    "cloudformation:ListStackResources",
```

```
    "cloudwatch:DeleteAlarms",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:GetMetricData",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "cloudwatch:PutMetricAlarm",
    "cloudwatch:PutMetricData",
    "codebuild:BatchGetBuilds",
    "codebuild:StartBuild",
    "codecommit:BatchGetRepositories",
    "codecommit:CreateRepository",
    "codecommit:GetRepository",
    "codecommit:List*",
    "codecommit:GitPull",
    "codecommit:GitPush",
    "ec2:CreateNetworkInterface",
    "ec2:CreateNetworkInterfacePermission",
    "ec2:DeleteNetworkInterface",
    "ec2:DeleteNetworkInterfacePermission",
    "ec2:DescribeDhcpOptions",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcEndpointServices",
    "ec2:DescribeVpcs",
    "ecr:BatchCheckLayerAvailability",
    "ecr:BatchGetImage",
    "ecr:CreateRepository",
    "ecr:Describe*",
    "ecr:GetAuthorizationToken",
    "ecr:GetDownloadUrlForLayer",
    "ecr:SetRepositoryPolicy",
    "ecr:CompleteLayerUpload",
    "ecr:BatchDeleteImage",
    "ecr:UploadLayerPart",
    "ecr:DeleteRepositoryPolicy",
    "ecr:InitiateLayerUpload",
    "ecr:DeleteRepository",
    "ecr:PutImage",
    "ecr:StartImageScan",
    "ecr:TagResource",
    "ecr:UntagResource",
```

```
    "elastic-inference:Connect",
    "elasticfilesystem:DescribeFileSystems",
    "elasticfilesystem:DescribeMountTargets",
    "elasticmapreduce:DescribeCluster",
    "elasticmapreduce:ListInstanceGroups",
    "elasticmapreduce:ListClusters",
    "events:PutRule",
    "events:DescribeRule",
    "events:PutTargets",
    "events:TagResource",
    "events:ListTagsForResource",
    "fsx:DescribeFileSystems",
    "glue:SearchTables",
    "glue:NotifyEvent",
    "glue:StartBlueprintRun",
    "glue:PutWorkflowRunProperties",
    "glue:StopCrawler",
    "glue:DeleteJob",
    "glue:DeleteWorkflow",
    "glue:UpdateCrawler",
    "glue:DeleteBlueprint",
    "glue:UpdateWorkflow",
    "glue:StartCrawler",
    "glue:ResetJobBookmark",
    "glue:UpdateJob",
    "glue:StartWorkflowRun",
    "glue:StopCrawlerSchedule",
    "glue:ResumeWorkflowRun",
    "glue:DeleteCrawler",
    "glue:UpdateBlueprint",
    "glue:BatchStopJobRun",
    "glue:StopWorkflowRun",
    "glue:BatchGet*",
    "glue:UpdateCrawlerSchedule",
    "glue:DeleteConnection",
    "glue:UpdateConnection",
    "glue:Get*",
    "glue:BatchDeleteConnection",
    "glue:StartCrawlerSchedule",
    "glue:StartJobRun",
    "glue:CreateWorkflow",
    "glue:*DataQuality*",
    "glue:List*",
    "glue:CreateSession",
```

```
    "glue:RunStatement",
    "glue:BatchCreatePartition",
    "glue:CreateDatabase",
    "glue:CreatePartitionIndex",
    "glue:CreateTable",
    "glue:BatchUpdatePartition",
    "glue:BatchDeletePartition",
    "glue:UpdateTable",
    "glue:DeleteTableVersion",
    "glue:DeleteTable",
    "glue:DeleteColumnStatisticsForPartition",
    "glue:DeleteColumnStatisticsForTable",
    "glue:DeletePartitionIndex",
    "glue:UpdateColumnStatisticsForPartition",
    "glue:UpdateColumnStatisticsForTable",
    "glue:BatchDeleteTableVersion",
    "glue:BatchDeleteTable",
    "glue:CreatePartition",
    "glue:DeletePartition",
    "glue:UpdatePartition",
    "glue:CreateBlueprint",
    "glue:CreateJob",
    "glue:CreateConnection",
    "glue:CreateCrawler",
    "groundtruthlabeling:*",
    "iam:CreateServiceLinkedRole",
    "iam:GetRole",
    "iam:ListRoles",
    "iam:PassRole",
    "kms:DescribeKey",
    "kms:ListAliases",
    "kms:Decrypt",
    "kms:ListKeys",
    "kms:Encrypt",
    "kms:GenerateDataKey",
    "kms:RetireGrant",
    "lakeformation:GetDataAccess",
    "lambda:ListFunctions",
    "lambda:InvokeFunction",
    "logs:CreateLogDelivery",
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:DeleteLogDelivery",
    "logs:Describe*",
```

```
    "logs:GetLogDelivery",
    "logs:GetLogEvents",
    "logs:ListLogDeliveries",
    "logs:PutLogEvents",
    "logs:UpdateLogDelivery",
    "ram:AcceptResourceShareInvitation",
    "rds:DescribeDBInstances",
    "redshift:CreateClusterUser",
    "redshift:GetClusterCredentials",
    "redshift:GetClusterCredentialsWithIAM",
    "redshift:DescribeClusters",
    "redshift-data:BatchExecuteStatement",
    "redshift-data:CancelStatement",
    "redshift-data:DescribeStatement",
    "redshift-data:DescribeTable",
    "redshift-data:ExecuteStatement",
    "redshift-data:GetStatementResult",
    "redshift-data:ListSchemas",
    "redshift-data:ListTables",
    "redshift-serverless:ListNamespaces",
    "redshift-serverless:ListWorkgroups",
    "redshift-serverless:GetNamespace",
    "redshift-serverless:GetWorkgroup",
    "redshift-serverless:GetCredentials",
    "s3:GetBucketAcl",
    "s3:PutObjectAcl",
    "s3:GetObject",
    "s3:PutObject",
    "s3:DeleteObject",
    "s3:AbortMultipartUpload",
    "s3:CreateBucket",
    "s3:GetBucketLocation",
    "s3:ListBucket",
    "s3:ListAllMyBuckets",
    "s3:GetBucketCors",
    "s3:PutBucketCors",
    "s3:DeleteObjectVersion",
    "s3:PutObjectRetention",
    "s3:ReplicateObject",
    "s3:RestoreObject",
    "secretsmanager:ListSecrets",
    "secretsmanager:DescribeSecret",
    "secretsmanager:GetSecretValue",
    "secretsmanager:CreateSecret",
```

```
    "secretsmanager:PutResourcePolicy",
    "secretsmanager:TagResource",
    "servicecatalog:Describe*",
    "servicecatalog:List*",
    "servicecatalog:ScanProvisionedProducts",
    "servicecatalog:SearchProducts",
    "servicecatalog:SearchProvisionedProducts",
    "servicecatalog:ProvisionProduct",
    "servicecatalog:TerminateProvisionedProduct",
    "servicecatalog:UpdateProvisionedProduct",
    "sns:ListTopics",
    "sns:Subscribe",
    "sns:CreateTopic",
    "sns:Publish",
    "states:DescribeExecution",
    "states:GetExecutionHistory",
    "states:StartExecution",
    "states:StopExecution",
    "states:UpdateStateMachine",
    "tag:GetResources",
    "sso:CreateApplicationAssignment",
    "sso:AssociateProfile"
   ],
   "Resource": "*"
  }
 ]
}
```

Amazon, AWS 관리형 정책 DataZone 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 DataZone 이후 Amazon의 AWS 관리형 정책 업데이트에 대한 세부 정보를 확인하십시오. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 Amazon DataZone Document 기록 페이지에서 RSS 피드를 구독하십시오.

변경 사항	설명	날짜
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary - 새 권한 경계	새 권한 경계가 AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary호출되었습니다.	2024년 4월 30일

변경 사항	설명	날짜
	Amazon DataZone 데이터 포털을 통해 Amazon SageMaker 환경을 생성하면 Amazon 은 환경 생성 중에 생성되는 IAM 역할에 이 권한 경계를 DataZone 적용합니다. 권한 경계는 Amazon이 DataZone 생성하는 역할 및 사용자가 추가하는 모든 역할의 범위를 제한합니다.	
AmazonDataZoneSageMakerAccess - 새 정책	라는 새 정책은 Amazon에 Amazon SageMaker 자산을 카탈로그에 게시할 수 있는 DataZone 권한을 AmazonDataZoneSageMakerAccess부여합니다. 또한 Amazon에 카탈로그에 SageMaker 게시된 자산에 대한 액세스 DataZone 권한을 부여하거나 액세스 권한을 취소할 수 있는 권한을 Amazon에 부여합니다.	2024년 4월 30일
AmazonDataZoneFullAccess - 정책 업데이트	콘솔에서 블루프린트를 구성하고 지정된 관리형 AmazonDataZoneFullAccess정책에 대한 정보를 검색하는 데 도움이 되는 `DescribeSecurityGroups` 작업을 구성하는 계정 관리자의 편의성을 개선하기 위해 `GetPolicy` 작업에 대한 액세스 권한을 추가하는 정책 업데이트입니다.	2024년 4월 30일

변경 사항	설명	날짜
AmazonDataZoneSage MakerProvisioning - 새 정책	Amazon이라는 새 정책은 DataZone Amazon과 상호 운용하는 데 필요한 권한을 SageMaker Amazon에 AmazonDataZoneSage MakerProvisioning부여합니다.	2024년 4월 30일
AmazonDataZone<domainId>S3관리- <region>- - 새 역할	AmazonDataZoneS3Manage-라는 새로운 역할 - <region><domainId>아마존이 AWS Lake Formation을 DataZone 호출하여 아마존 심플 스토리지 서비스 (Amazon S3) 의 위치를 등록할 때 사용됩니다. AWS Lake Formation은 해당 위치의 데이터에 액세스할 때 이 역할을 맡습니다.	2024년 4월 1일
AmazonDataZoneGlue ManageAccessRolePolicy - 정책 업데이트	Amazon이 AmazonDataZoneGlueManageAccessRolePolicy데이터에 대한 게시 및 액세스 권한 DataZone 부여를 활성화할 수 있는 권한에 대한 지원을 활성화하도록 업데이트되었습니다.	2024년 4월 1일
AmazonDataZoneDomainExecutionRolePolicy 및 AmazonDataZoneFullUserAccess - 정책 업데이트	`CancelMetadataGenerationRun` API에 대한 지원을 AmazonDataZoneFullUserAccess활성화하도록 AmazonDataZoneDomainExecutionRolePolicy및 를 업데이트했습니다.	2024년 3월 29일

변경 사항	설명	날짜
AmazonDataZoneFullAccess - 정책 업데이트	사용자가 텍스트 상자에 입력하지 않고 Amazon DataZone 관리 콘솔에서 암호, 클러스터, vpc 및 서브넷을 선택할 수 있도록 업데이트되었습니다. `AmazonDataZoneFullAccess`	2024년 3월 13일
AmazonDataZoneDomainExecutionRolePolicy - 정책 업데이트	어떤 계정과 지역에서 어떤 블루프린트가 활성화되었는지 식별하여 환경 프로필 생성에 필요한 `ListEnvironmentBlueprintConfigurationSummaries` API를 지원할 수 있도록 업데이트되었습니다. AmazonDataZoneDomainExecutionRolePolicy	2024년 2월 1일
AmazonDataZoneGlueManageAccessRolePolicy - 정책 업데이트	AWS Lake Formation 하이브리드 모드를 지원할 수 AmazonDataZoneGlueManageAccessRolePolicy있도록 업데이트되었습니다.	2023년 12월 14일
AmazonDataZoneFullUserAccess 및 AmazonDataZoneDomainExecutionRolePolicy - 정책 업데이트	Amazon에서 AI 기반 데이터 설명 생성 기능을 지원하도록 AmazonDataZoneFullUserAccess및 AmazonDataZoneDomainExecutionRolePolicy정책을 업데이트했습니다. DataZone	2023년 11월 28일

변경 사항	설명	날짜
AmazonDataZoneEnvironmentRolePermissionsBoundary - 정책 업데이트	DataZone Amazon은 `ResourceTag` 조건에 따라 범위가 축소된 추가 `athena:GetQueryResultsStream` 권한으로 구성된 AmazonDataZoneEnvironmentRolePermissionsBoundary관리형 정책을 업데이트했습니다.	2023년 11월 17일
AmazonDataZoneRedshiftManageAccessRolePolicy - 정책 업데이트	Amazon은 해당 `redshift:AssociateDataShareConsumer` 작업에 대한 조직 ID 확인을 AmazonDataZoneRedshiftManageAccessRolePolicy제거하여 DataZone 업데이트했습니다. 이렇게 하면 AWS 조직 간에 리소스를 공유할 수 있습니다.	2023년 11월 16일
AmazonDataZoneFullUserAccess - 정책 업데이트	Amazon은 DataZone Amazon에 대한 전체 액세스 권한을 부여하는 AmazonDataZoneFullUserAccess정책을 DataZone 업데이트했지만 도메인, 사용자 또는 관련 계정의 관리는 허용하지 않습니다.	2023년 10월 2일
AmazonDataZonePortalFullAccessPolicy - 정책이 더 이상 사용되지 않음	Amazon은 DataZone 더 이상 사용되지 않습니다. AmazonDataZonePortalFullAccessPolicy	2023년 9월 29일

변경 사항	설명	날짜
AmazonDataZonePrev iewConsoleFullAccess - 정책이 더 이상 사용되지 않음	Amazon은 DataZone 더 이상 사용되지 않습니다. AmazonDataZonePrev iewConsoleFullAccess	2023년 9월 29일
AmazonDataZoneDoma inExecutionRolePolicy - 새 정책	Amazon은 이라는 새 정책을 DataZone 추가했습니다 AmazonDataZoneDoma inExecutionRolePolicy. Amazon DataZone `AmazonDataZoneDoma inExecutionRole` 서비스 역할의 기본 정책입니다. Amazon은 이 역할을 DataZone 사용하여 Amazon DataZone 도메인의 데이터를 카탈로그, 검색, 관리, 공유 및 분석합니다. 정책을 귀하의 `AmazonDat aZoneDomainExecuti onRolePolicy` `AmazonDataZoneDoma inExecutionRole` 정책에 첨부할 수 있습니다.	2023년 9월 25일
AmazonDataZoneCros sAccountAdmin - 새 정책	Amazon은 사용자가 Amazon DataZone 및 관련 계정을 사용할 수 있도록 하는 새로운 정책을 DataZone 추가했습니다. AmazonDataZoneCros sAccountAdmin	2023년 9월 19일

변경 사항	설명	날짜
AmazonDataZoneFull UserAccess - 새 정책	Amazon은 DataZone Amazon에 대한 전체 액세스 권한을 부여하는 AmazonDataZoneFull UserAccess정책이라는 새 정책을 DataZone 추가했지만 도메인, 사용자 또는 관련 계정의 관리는 허용하지 않습니다.	2023년 9월 12일
AmazonDataZoneRedshiftManageAccessRolePolicy - 새 정책	Amazon은 AmazonDataZoneRedshiftManageAccessRolePolicyAmazon이 데이터에 대한 게시 및 액세스 권한을 DataZone 허용할 수 있는 권한을 부여하는 새 정책을 DataZone 추가했습니다.	2023년 9월 12일
AmazonDataZoneGlueManageAccessRolePolicy - 새 정책	Amazon은 AWS Glue 데이터를 카탈로그에 게시할 DataZone 권한을 Amazon에 AmazonDataZoneGlueManageAccessRolePolicy부여하는 새 정책을 DataZone 추가했습니다. 또한 Amazon에 카탈로그에 있는 AWS Glue 게시 자산에 대한 액세스 DataZone 권한을 부여하거나 액세스 권한을 취소할 수 있는 권한을 부여합니다.	2023년 9월 12일

변경 사항	설명	날짜
AmazonDataZoneRedshiftGlueProvisioningPolicy - 새 정책	Amazon은 지원되는 데이터 소스와 상호 AmazonDataZoneRedshiftGlueProvisioningPolicy운용하는 데 필요한 권한을 DataZone Amazon에 부여하는 새 정책을 DataZone 추가했습니다.	2023년 9월 12일
AmazonDataZoneEnvironmentRolePermissionsBoundary - 새 정책	Amazon은 연결된 프로비저닝된 IAM 보안 주체를 제한하는 새 정책을 DataZone 추가했습니다. AmazonDataZoneEnvironmentRolePermissionsBoundary	2023년 9월 12일
AmazonDataZoneFullAccess - 새 정책	Amazon은 AWS 관리 콘솔을 DataZone 통해 Amazon에 대한 전체 액세스를 AmazonDataZoneFullAccess제공하는 새로운 정책을 DataZone 추가했습니다.	2023년 9월 12일
관리형 정책 업데이트	추가 `iam:GetPolicy` 권한으로 구성된 AmazonDataZonePreviewConsoleFullAccess관리형 정책 업데이트.	2023년 6월 13일
Amazon은 변경 사항 추적을 DataZone 시작했습니다	Amazon은 AWS 관리형 정책의 변경 사항을 추적하기 DataZone 시작했습니다.	2023년 3월 20일

아마존의 IAM 역할 DataZone

주제

- AmazonDataZoneProvisioningRole-<domainAccountId>
- AmazonDataZoneDomainExecutionRole
- AmazonDataZoneGlueAccess- <region>- <domainId>
- AmazonDataZoneRedshiftAccess- <region>- <domainId>
- AmazonDataZone<region>S3Manage- - <domainId>
- AmazonDataZoneSageMakerManageAccessRole<region>- - <domainId>
- AmazonDataZoneSageMakerProvisioningRole-<domainAccountId>

AmazonDataZoneProvisioningRole-<domainAccountId>

`AmazonDataZoneProvisioningRole-<domainAccountId>``AmazonDataZoneRedshiftGlueProvisioningPolicy`첨부된 내용이 있습니다. 이 역할은 DataZone Amazon에 AWS Glue 및 Amazon Redshift와 상호 운용하는 데 필요한 권한을 부여합니다.

`AmazonDataZoneProvisioningRole-<domainAccountId>`기본값에는 다음과 같은 신뢰 정책이 첨부되어 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "datazone.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "{{domain_account}}"
        }
      }
    }
  ]
}
```

AmazonDataZoneDomainExecutionRole

AmazonDataZoneDomainExecutionRole에는 AWS 관리형 정책이 AmazonDataZoneDomainExecutionRolePolicy첨부되어 있습니다. DataZone Amazon은 귀하를 대신하여 이 역할을 생성합니다. 데이터 포털의 특정 작업에 대해 Amazon은 역할이 생성된 계정에서 이 역할을 DataZone 맡고 이 역할이 작업을 수행할 권한이 있는지 확인합니다.

Amazon DataZone 도메인을 AWS 계정 호스팅하는 AmazonDataZoneDomainExecutionRole역할을 수행해야 합니다. 이 역할은 Amazon DataZone 도메인을 생성할 때 자동으로 생성됩니다.

기본 AmazonDataZoneDomainExecutionRole역할에는 다음과 같은 신뢰 정책이 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "datazone.amazonaws.com"
            },
            "Action": [
                "sts:AssumeRole",
                "sts:TagSession"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "{{source_account_id}}"
                },
                "ForAllValues:StringLike": {
                    "aws:TagKeys": [
                        "datazone*"
                    ]
                }
            }
        }
    ]
}
```

AmazonDataZoneGlueAccess- <region>- <domainId>

AmazonDataZoneGlueAccess-<region>-<domainId>역할이 AmazonDataZoneGlueManageAccessRolePolicy 첨부되어 있습니다. 이 역할은 Amazon에 AWS Glue 데이터를 카탈로그에 게시할 DataZone 권한을 부여합니다. 또한 Amazon에 카탈로그에 있는 AWS Glue 게시 자산에 대한 액세스 DataZone 권한을 부여하거나 액세스 권한을 취소할 수 있는 권한을 부여합니다.

기본 AmazonDataZoneGlueAccess-<region>-<domainId> 역할에는 다음과 같은 신뢰 정책이 첨부되어 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "datazone.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "{{domain_account}}"
            },
            "ArnEquals": {
                "aws:SourceArn": "arn:aws:datazone:{{region}}:
{{domain_account}}:domain/{{root_domain_id}}"
            }
        }
    }
  ]
}
```

AmazonDataZoneRedshiftAccess- <region>- <domainId>

AmazonDataZoneRedshiftAccess-<region>-<domainId>역할이 AmazonDataZoneRedshiftManageAccessRolePolicy 첨부되어 있습니다. 이 역할은 Amazon Redshift 데이터를 카탈로그에 게시할 DataZone 권한을 Amazon에 부여합니다. 또한 카탈로그에 있는

Amazon Redshift 또는 Amazon Redshift 서버리스에 게시된 자산에 대한 액세스 DataZone 권한을 부여하거나 액세스 권한을 취소할 수 있는 권한을 아마존에 부여합니다.

기본 AmazonDataZoneRedshiftAccess-<region>-<domainId> 역할에는 다음과 같은 인라인 권한 정책이 첨부되어 있습니다.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "RedshiftSecretStatement",
         "Effect":"Allow",
         "Action":"secretsmanager:GetSecretValue",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "secretsmanager:ResourceTag/AmazonDataZoneDomain":"{{domainId}}"
            }
         }
      }
   ]
}
```

AmazonDataZoneRedshiftManageAccessRole<timestamp>기본값에는 다음과 같은 신뢰 정책이 첨부되어 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "datazone.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "{{domain_account}}"
            },
```

```
            "ArnEquals": {
                "aws:SourceArn": "arn:aws:datazone:{{region}}:
{{domain_account}}:domain/{{root_domain_id}}"
            }
        }
    }
  ]
}
```

AmazonDataZone<region>S3Manage- - <domainId>

AmazonDataZoneS3Manage- <region>- <domainId>는 아마존이 AWS Lake Formation을 DataZone 호출하여 아마존 심플 스토리지 서비스 (Amazon S3) 의 위치를 등록할 때 사용됩니다. AWS Lake Formation은 해당 위치의 데이터에 액세스할 때 이 역할을 맡습니다. 자세한 내용은 위치 등록에 사용되는 역할 요구 사항을 참조하십시오.

이 역할에는 다음과 같은 인라인 권한 정책이 첨부되어 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "LakeFormationDataAccessPermissionsForS3",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{accountId}}"
                }
            }
        },
        {
            "Sid": "LakeFormationDataAccessPermissionsForS3ListBucket",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
```

```
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{accountId}}"
                }
            }
        },
        {
            "Sid": "LakeFormationDataAccessPermissionsForS3ListAllMyBuckets",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "arn:aws:s3:::*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{accountId}}"
                }
            }
        },
        {
            "Sid": "LakeFormationExplicitDenyPermissionsForS3",
            "Effect": "Deny",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::[[BucketNames]]/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{accountId}}"
                }
            }
        },
        {
            "Sid": "LakeFormationExplicitDenyPermissionsForS3ListBucket",
            "Effect": "Deny",
            "Action": [
                "s3:ListBucket"
            ],
```

```
            "Resource": [
                "arn:aws:s3:::[[BucketNames]]"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{accountId}}"
                }
            }
        }
    ]
}
```

AmazonDataZoneS3Manage- <region>- <domainId>에는 다음과 같은 신뢰 정책이 첨부되어 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TrustLakeFormationForDataLocationRegistration",
            "Effect": "Allow",
            "Principal": {
                "Service": "lakeformation.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "{{source_account_id}}"
                }
            }
        }
    ]
}
```

AmazonDataZoneSageMakerManageAccessRole<region>- - <domainId>

AmazonDataZoneSageMakerManageAccessRole역할에는 'AmazonDataZoneSageMakerAccess,'AmazonDataZoneRedshiftManageAccessRolePolicy, AmazonDataZoneGlueManageAccessRolePolicy '첨부'가 있습니다. 이 역할은 Amazon에 데이터

레이크, 데이터 웨어하우스 및 Amazon Sagemaker 자산에 대한 구독을 게시하고 관리할 DataZone 권한을 부여합니다.

AmazonDataZoneSageMakerManageAccessRole역할에는 다음과 같은 인라인 정책이 첨부되어 있습니다.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "RedshiftSecretStatement",
         "Effect":"Allow",
         "Action":"secretsmanager:GetSecretValue",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "secretsmanager:ResourceTag/AmazonDataZoneDomain":"{{domainId}}"
            }
         }
      }
   ]
}
```

AmazonDataZoneSageMakerManageAccessRole역할에는 다음과 같은 신뢰 정책이 첨부되어 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DatazoneTrustPolicyStatement",
      "Effect": "Allow",
      "Principal": {
        "Service":  ["datazone.amazonaws.com",
                    "sagemaker.amazonaws.com"]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
            "StringEquals": {
```

```
                "aws:SourceAccount": "{{domain_account}}"
            },
            "ArnEquals": {
                "aws:SourceArn": "arn:aws:datazone:{{region}}:
{{domain_account}}:domain/{{root_domain_id}}"
            }
        }
    }
]
}
```

AmazonDataZoneSageMakerProvisioningRole-<domainAccountId>

AmazonDataZoneSageMakerProvisioningRole역할에는 AmazonDataZoneSageMakerProvisioning 와 가 AmazonDataZoneRedshiftGlueProvisioningPolicy 첨부되어 있습니다. 이 역할은 AWS Glue, Amazon Redshift 및 Amazon Sagemaker와 상호 운용하는 데 필요한 DataZone 권한을 아마존에 부여합니다.

AmazonDataZoneSageMakerProvisioningRole역할에는 다음과 같은 인라인 정책이 첨부되어 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SageMakerStudioTagOnCreate",
            "Effect": "Allow",
            "Action": [
                "sagemaker:AddTags"
            ],
            "Resource": "arn:aws:sagemaker:*:{{AccountId}}:*/*",
            "Condition": {
                "Null": {
                    "sagemaker:TaggingAction": "false"
                }
            }
        }
    ]
}
```

AmazonDataZoneSageMakerProvisioningRole역할에는 다음과 같은 신뢰 정책이 첨부되어 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DataZoneTrustPolicyStatement",
      "Effect": "Allow",
      "Principal": {
        "Service": "datazone.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "{{domain_account}}"
        }
      }
    }
  ]
}
```

ID 기반 역할

자격 증명 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는 지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

IAM 자격 증명 기반 정책을 사용하면 허용되거나 거부되는 작업와 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. 자격 증명 기반 정책에서는 보안 주체가 연결된 사용자 또는 역할에 적용되므로 보안 주체를 지정할 수 없습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

Amazon DataZone 프로젝트를 생성하면 포털에서 이 프로젝트에 대해 소유자 및 기여자별로 프로젝트 구성원 역할 유형별로 하나씩 총 3개의 IAM 역할이 생성됩니다. 각 역할에 부여된 권한의 범위는 프로젝트 역할로 제한되며, 연결된 권한 정책은 프로젝트가 배포되는 기능에 따라 달라집니다.

Amazon이 DataZone 권한을 관리하고 구독자 프로젝트와 자산을 공유할 수 있도록 구독자 프로젝트 사용자 역할은 자산 게시 시 데이터 레이크 관리자로 자동 추가됩니다. AWS Lake Formation AWS 계정

AWS IAM 관리 콘솔에서 대부분의 역할 up-to-date 버전을 보거나 아래 표에서 다양한 역할 권한을 검토할 수 있습니다.

프로젝트 소유자 권한

환경 유형	IAM 권한
기본 데이터 레이크	이는 에센셜, 데이터 레이크 프로듀서 및 데이터 레이크 컨슈머 기능의 조합입니다.
Essential	{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["s3:List*", "s3:Get*", "s3:Describe*", "s3:DeleteObjectVersion", "s3:RestoreObject", "s3:ReplicateObject", "s3:PutObject", "s3:AbortMultipartUpload", "s3:PutObjectRetention", "s3:DeleteObject"], "Resource": ["s3BucketArn", "s3BucketArn/*"]

환경 유형	IAM 권한	
	}, { "Action": ["s3:List*"], "Resource": "*", "Effect": "Allow" }, { "Action": ["kms:List*", "kms:Get*", "kms:Describe*", "kms:Decrypt", "kms:Encrypt", "kms:ReEncrypt*", "kms:Verify", "kms:Sign", "kms:GenerateDataKey"], "Resource": "keyArn", "Effect": "Allow" }, { "Action": ["kms:ListKeys", "kms:ListAliases"], "Resource": "*", "Effect": "Allow" }, { "Action": ["ec2:DescribeSecurityGroups", "ec2:DescribeSecurityGroupRules", "ec2:DescribeTags"], "Resource": "*",	

환경 유형	IAM 권한	

```
      "Effect": "Allow"
    },
    {
      "Action": [
        "logs:Des
cribe*",
        "logs:Sta
rtQuery",
        "logs:Sto
pQuery",
        "logs:Get*",
        "logs:List*",
        "logs:Put
LogEvents",
        "logs:Cre
ateLogStream",
        "logs:Fil
terLogEvents"
      ],
      "Resource":
 "arn:aws:logs:regi
on:account-id:log-
group:log-group-na
me:*",
      "Effect": "Allow"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "kms:List*",
        "kms:Get*",
        "kms:Desc
ribe*",
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringNo
tEquals": {
```

환경 유형	IAM 권한	
	"aws:Reso urceAccount": "project-account-id" } } }] }	

환경 유형	IAM 권한	
데이터 레이크 프로듀서	{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["glue:BatchGet*", "glue:Get*", "glue:SearchTables", "glue:List*", "glue:BatchCreatePartition", "glue:CreatePartitionIndex", "glue:CreateTable", "glue:BatchUpdatePartition", "glue:BatchDeletePartition", "glue:UpdateTable", "glue:DeleteTableVersion", "glue:DeleteTable", "glue:DeleteColumn	

환경 유형	IAM 권한	

```
StatisticsForParti
tion",

 "glue:DeleteColumn
StatisticsForTable",

 "glue:DeletePartit
ionIndex",

 "glue:UpdateColumn
StatisticsForParti
tion",

 "glue:UpdateColumn
StatisticsForTable",

 "glue:BatchDeleteT
ableVersion",

 "glue:BatchDeleteT
able",

 "glue:CreatePartit
ion",

 "glue:DeletePartit
ion",

 "glue:UpdatePartit
ion"
            ],
            "Resource":
 [

 "arn:aws:glue:regi
on:account:database/
dbName",

 "arn:aws:glue:regi
on:account:catalog",

 "arn:aws:glue:regi
```

환경 유형	IAM 권한	

```
on:account:table/d
bName/*"
            ]
        },
        {
            "Sid":
 "VisualEditor0",
            "Effect":
 "Allow",
            "Action": [

 "glue:SearchTables",

 "glue:NotifyEvent",

 "glue:StartBluepri
ntRun",

 "glue:PutWorkflowR
unProperties",

 "glue:StopCrawler",

 "glue:DeleteJob",

 "glue:DeleteWorkfl
ow",

 "glue:UpdateCrawler",

 "glue:DeleteBluepr
int",

 "glue:UpdateWorkfl
ow",

 "glue:StartCrawler",

 "glue:ResetJobBook
mark",

 "glue:UpdateJob",
```

환경 유형	IAM 권한	
	"glue:StartWorkflowRun", "glue:StopCrawlerSchedule", "glue:ResumeWorkflowRun", "glue:List*", "glue:DeleteCrawler", "glue:UpdateBlueprint", "glue:BatchStopJobRun", "glue:StopWorkflowRun", "glue:BatchGet*", "glue:UpdateCrawlerSchedule", "glue:DeleteConnection", "glue:UpdateConnection", "glue:Get*", "glue:BatchDeleteConnection", "glue:StartCrawlerSchedule",	

환경 유형	IAM 권한	

```
 "glue:StartJobRun",

 "glue:CreateWorkfl
ow",

 "glue:PublishDataQ
uality",

 "glue:*DataQuality*"
           ],
           "Resource":
 "*",
           "Conditio
n": {

 "ForAnyValue:Strin
gEquals": {

 "aws:ResourceTag/n
oah-analytics:proj
ectId": "projectId"
               }
           }
       },
       {
           "Sid":
 "CreateGlueResourc
es",
           "Effect":
 "Allow",
           "Action": [

 "glue:CreateBluepr
int",

 "glue:CreateJob",

 "glue:CreateConnec
tion",

 "glue:CreateCrawler",
```

환경 유형	IAM 권한	

```
 "glue:CreateDataQu
alityRuleset"
            ],
            "Resource":
 "*"
        },
        {
            "Sid":
 "VisualEditor0",
            "Effect":
 "Allow",
            "Action": [

 "iam:ListRoles",

 "iam:ListUsers",

 "iam:ListGroups",

 "iam:ListRolePolic
ies",

 "iam:GetRole",

 "iam:GetRolePolicy"
            ],
            "Resource":
 "*"
        }
    ]
}
```

환경 유형	IAM 권한	
데이터 레이크 소비자	{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["athena:TerminateSession", "athena:CreatePreparedStatement", "athena:StopCalculationExecution", "athena:StartQueryExecution", "athena:UpdatePreparedStatement", "athena:BatchGet*", "athena:UpdateNotebook", "athena:DeleteNotebook", "athena:DeletePreparedStatement", "athena:UpdateNotebookMetadata", "athena:DeleteNamedQuery", "athena:Get*", "athena:UpdateNamedQuery", "athena:CreateNamedQuery",	

환경 유형	IAM 권한	

```
        "athena:E
xportNotebook",
        "athena:S
topQueryExecution",
        "athena:S
tartCalculationExe
cution",
        "athena:S
tartSession",
        "athena:C
reatePresignedNote
bookUrl",
        "athena:C
reateNotebook",
        "athena:I
mportNotebook"
      ],
      "Resource": [
        "arn:aws:
athena:region:acco
unt-id:workgroup/w
orkGroupName",
        "arn:aws:
athena:region:acco
unt-id:datacatalog/
AwsDataCatalog"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "athena:L
istWorkGroups",
        "athena:L
istDataCatalogs",
        "athena:List*"
      ],
      "Resource": ["*"]
    },
    {
      "Effect": "Allow",
      "Action": [
```

환경 유형	IAM 권한	
	"glue:Bat chGet*", "glue:Get*", "glue:Sea rchTables", "glue:List*"], "Resource": ["arn:aws: glue:region:account- id:database/dbName", "arn:aws: glue:region:account- id:catalog", "arn:aws: glue:region:account- id:table/dbName/*"] }] }	

환경 유형	IAM 권한	

데이터 웨어하우스 프로듀서	{
	  "Version": "2012-10-17",
	  "Statement": [
	  {
	  "Effect": "Allow",
	  "Action": [
	  "redshift:GetClusterCredentials",
	  "redshift:JoinGroup",
	  "redshift:CreateClusterUser",
	  "redshift:DescribeClusters"
	  ],
	  "Resource": "arn:aws:redshift:region:account:cluster:producerRedshiftCluster"
	  },
	  {
	  "Effect": "Allow",
	  "Action": [
	  "redshift-data:DescribeStatement",
	  "redshift-data:ExecuteStatement"
	  ],
	  "Resource": "arn:aws:redshift:region:account:cluster:producerRedshiftCluster"
	  }
	  ]
	}	

환경 유형	IAM 권한	

환경 유형	IAM 권한	

데이터 웨어하우스 소비자	{
	"Version": "2012-10-17",
	"Statement": [
	{
	"Effect": "Allow",
	"Action": [
	"redshift:GetClusterCredentials",
	"redshift:JoinGroup",
	"redshift:CreateClusterUser",
	"redshift:DescribeClusters"
	],
	"Resource": [
	"arn:aws:redshift:region:account:dbuser:cluster-identifier/dbUser",
	"arn:aws:redshift:region:account:dbgroup:cluster-identifier/project_owner@projectName",
	"arn:aws:redshift:region:account:dbname:cluster-identifier/*"
	],
	"Condition": {
	"ForAnyValue:StringEquals": {
	"aws:PrincipalTag/RedshiftDbUser": "dbUser"
	}	

환경 유형	IAM 권한	

```
      }
    },
    {
      "Sid": "VisualEd
itor2",
      "Effect": "Allow",
      "Action": [
        "redshift-
data:DescribeStat
ement",
        "redshift-
data:ExecuteStatement"
      ],
      "Resource":
 "arn:aws:redshift:
region:account-id:
cluster:cluster-id
entifier"
    }
  ]
}
```

환경 유형	IAM 권한	

Amazon Redshift 쿼리 편집기 v2	{
	"Version": "2012-10-17",
	"Statement": [
	{
	"Action": "redshift:DescribeClusters",
	"Effect": "Allow",
	"Resource": "arn:aws:redshift:region:account-id:cluster:*",
	"Sid": "RedshiftPermissions"
	},
	{
	"Action": "tag:GetResources",
	"Condition": {
	"StringEquals": { "aws:CalledViaLast": "sqlworkbench.amazonaws.com" }
	},
	"Effect": "Allow",
	"Resource": "*",
	"Sid": "ResourceGroupsTaggingPermissions"
	},
	{
	"Action": [
	"sqlworkbench:DriverExecute",
	"sqlworkbench:GenerateSession",	

환경 유형	IAM 권한	

```
        "sqlworkb
ench:ListConnectio
ns",
        "sqlworkb
ench:ListDatabases",
        "sqlworkb
ench:ListFiles",
        "sqlworkb
ench:ListNotebooks",
        "sqlworkb
ench:ListQueryExec
utionHistory",
        "sqlworkb
ench:ListRedshiftC
lusters",
        "sqlworkb
ench:ListSampleDat
abases",
        "sqlworkb
ench:ListTabs",
        "sqlworkb
ench:ListTaggedRes
ources"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Sid": "AmazonRe
dshiftQueryEditorV
2PermissionsPart1"
    },
    {
      "Action":
 "sqlworkbench:*",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:
sqlworkbench:regio
n:account-id:query/
*",
        "arn:aws:
sqlworkbench:regio
```

환경 유형	IAM 권한	
	n:account-id:notebook/*", "arn:aws:sqlworkbench:region:account-id:connection/*", "arn:aws:sqlworkbench:region:account-id:chart/*", "arn:aws:sqlworkbench:region:account-id:/*"], "Sid": "AmazonRedshiftQueryEditorV2PermissionsPart2" }] }	

프로젝트 기여자 권한

환경 유형	IAM 권한	
기본 데이터 레이크	이는 에센셜, 데이터 레이크 프로듀서 및 데이터 레이크 컨슈머 기능의 조합입니다.	
Essential	{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": [	

환경 유형	IAM 권한	

```
        "s3:List*",
        "s3:Get*",
        "s3:Describe*",
        "s3:Delet
eObjectVersion",
        "s3:Resto
reObject",
        "s3:Repli
cateObject",
        "s3:PutObject",
        "s3:Abort
MultipartUpload",
        "s3:PutOb
jectRetention",
        "s3:Delet
eObject"
      ],
      "Resource":
 ["s3BucketArn",
 "s3BucketArn/*"]
    },
    { "Action":
 ["s3:List*"],
 "Resource": "*",
 "Effect": "Allow" },
    {
      "Action": [
        "kms:List*",
        "kms:Get*",
        "kms:Desc
ribe*",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:ReEn
crypt*",
        "kms:Verify",
        "kms:Sign",
        "kms:Gene
rateDataKey"
      ],
      "Resource":
 "keyArn",
```

환경 유형	IAM 권한	

```
      "Effect": "Allow"
    },
    {
      "Action":
 ["kms:ListKeys",
 "kms:ListAliases"],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "ec2:Desc
ribeSecurityGroups",
        "ec2:Desc
ribeSecurityGroupR
ules",
        "ec2:Desc
ribeTags"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "logs:Des
cribe*",
        "logs:Sta
rtQuery",
        "logs:Sto
pQuery",
        "logs:Get*",
        "logs:List*",
        "logs:Put
LogEvents",
        "logs:Cre
ateLogStream",
        "logs:Fil
terLogEvents"
      ],
      "Resource":
 "arn:aws:logs:regi
on:account-id:log-
```

환경 유형	IAM 권한	

```
group:log-group-na
me:*",
      "Effect": "Allow"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "kms:List*",
        "kms:Get*",
        "kms:Desc
ribe*",
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringNo
tEquals": {
          "aws:Reso
urceAccount":
 "project-account-id"
        }
      }
    }
  ]
}
```

환경 유형	IAM 권한	
데이터 레이크 프로듀서	{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["glue:BatchGet*", "glue:Get*", "glue:SearchTables", "glue:List*", "glue:BatchCreatePartition", "glue:CreatePartitionIndex", "glue:CreateTable", "glue:BatchUpdatePartition", "glue:BatchDeletePartition", "glue:UpdateTable", "glue:DeleteTableVersion", "glue:DeleteTable", "glue:DeleteColumnStatisticsForPartition", "glue:DeleteColumnStatisticsForTable", "glue:DeletePartitionIndex", "glue:UpdateColumnStatisticsForPartition",	

환경 유형	IAM 권한	

```
        "glue:Upd
ateColumnStatistic
sForTable",
        "glue:Bat
chDeleteTableVersi
on",
        "glue:Bat
chDeleteTable",
        "glue:Cre
atePartition",
        "glue:Del
etePartition",
        "glue:Upd
atePartition"
      ],
      "Resource": [
        "arn:aws:
glue:region:accoun
t:database/dbName",
        "arn:aws:
glue:region:accoun
t:catalog",
        "arn:aws:
glue:region:accoun
t:table/dbName/*"
      ]
    },
    {
      "Sid": "VisualEd
itor0",
      "Effect": "Allow",
      "Action": [
        "glue:Sea
rchTables",
        "glue:Not
ifyEvent",
        "glue:Sta
rtBlueprintRun",
        "glue:Put
WorkflowRunPropert
ies",
```

환경 유형	IAM 권한	

```
        "glue:Sto
pCrawler",
        "glue:Del
eteJob",
        "glue:Del
eteWorkflow",
        "glue:Upd
ateCrawler",
        "glue:Del
eteBlueprint",
        "glue:Upd
ateWorkflow",
        "glue:Sta
rtCrawler",
        "glue:Res
etJobBookmark",
        "glue:Upd
ateJob",
        "glue:Sta
rtWorkflowRun",
        "glue:Sto
pCrawlerSchedule",
        "glue:Res
umeWorkflowRun",
        "glue:List*",
        "glue:Del
eteCrawler",
        "glue:Upd
ateBlueprint",
        "glue:Bat
chStopJobRun",
        "glue:Sto
pWorkflowRun",
        "glue:Bat
chGet*",
        "glue:Upd
ateCrawlerSchedule",
        "glue:Del
eteConnection",
        "glue:Upd
ateConnection",
        "glue:Get*",
```

환경 유형	IAM 권한	

```
        "glue:Bat
chDeleteConnection",
        "glue:Sta
rtCrawlerSchedule",
        "glue:Sta
rtJobRun",
        "glue:Cre
ateWorkflow",
        "glue:Pub
lishDataQuality",
        "glue:*Da
taQuality*"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyVa
lue:StringEquals": {
          "aws:Reso
urceTag/noah-analy
tics:projectId":
 "projectId"
        }
      }
    },
    {
      "Sid": "CreateGl
ueResources",
      "Effect": "Allow",
      "Action": [
        "glue:Cre
ateBlueprint",
        "glue:Cre
ateJob",
        "glue:Cre
ateConnection",
        "glue:Cre
ateCrawler",
        "glue:Cre
ateDataQualityRule
set"
      ],
      "Resource": "*"
```

환경 유형	IAM 권한	

```
    },
    {
      "Sid": "VisualEd
itor0",
      "Effect": "Allow",
      "Action": [
        "iam:List
Roles",
        "iam:List
Users",
        "iam:List
Groups",
        "iam:List
RolePolicies",
        "iam:GetRole",
        "iam:GetR
olePolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

환경 유형	IAM 권한	
데이터 레이크 소비자	{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["athena:TerminateSession", "athena:CreatePreparedStatement", "athena:StopCalculationExecution", "athena:StartQueryExecution", "athena:UpdatePreparedStatement", "athena:BatchGet*", "athena:UpdateNotebook", "athena:DeleteNotebook", "athena:DeletePreparedStatement", "athena:UpdateNotebookMetadata", "athena:DeleteNamedQuery", "athena:Get*", "athena:UpdateNamedQuery", "athena:CreateNamedQuery",	

환경 유형	IAM 권한	

```
        "athena:E
xportNotebook",
        "athena:S
topQueryExecution",
        "athena:S
tartCalculationExe
cution",
        "athena:S
tartSession",
        "athena:C
reatePresignedNote
bookUrl",
        "athena:C
reateNotebook",
        "athena:I
mportNotebook"
      ],
      "Resource": [
        "arn:aws:
athena:region:acco
unt-id:workgroup/w
orkGroupName",
        "arn:aws:
athena:region:acco
unt-id:datacatalog/
AwsDataCatalog"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "athena:L
istWorkGroups",
        "athena:L
istDataCatalogs",
        "athena:List*"
      ],
      "Resource": ["*"]
    },
    {
      "Effect": "Allow",
      "Action": [
```

환경 유형	IAM 권한	

```
        "glue:Bat
chGet*",
        "glue:Get*",
        "glue:Sea
rchTables",
        "glue:List*"
      ],
      "Resource": [
        "arn:aws:
glue:region:account-
id:database/dbName",
        "arn:aws:
glue:region:account-
id:catalog",
        "arn:aws:
glue:region:account-
id:table/dbName/*"
      ]
    }
  ]
}
```

환경 유형	IAM 권한	

데이터 웨어하우스 프로듀서	{
	  "Version": "2012-10-17",
	  "Statement": [
	    {
	      "Effect": "Allow",
	      "Action": [
	        "redshift:GetClusterCredentials",
	        "redshift:JoinGroup",
	        "redshift:CreateClusterUser",
	        "redshift:DescribeClusters"
	      ],
	      "Resource": "arn:aws:redshift:region:account:cluster:producerRedshiftCluster"
	    },
	    {
	      "Effect": "Allow",
	      "Action": [
	        "redshift-data:DescribeStatement",
	        "redshift-data:ExecuteStatement"
	      ],
	      "Resource": "arn:aws:redshift:region:account:cluster:producerRedshiftCluster"
	    }
	  ]
	}	

환경 유형	IAM 권한	

환경 유형	IAM 권한	

데이터 웨어하우스 소비자	{
	"Version": "2012-10-17",
	"Statement": [
	{
	"Effect": "Allow",
	"Action": [
	"redshift:GetClusterCredentials",
	"redshift:JoinGroup",
	"redshift:CreateClusterUser",
	"redshift:DescribeClusters"
	],
	"Resource": [
	"arn:aws:redshift:region:account:dbuser:cluster-identifier/dbUser",
	"arn:aws:redshift:region:account:dbgroup:cluster-identifier/project_owner@projectName",
	"arn:aws:redshift:region:account:dbname:cluster-identifier/*"
	],
	"Condition": {
	"ForAnyValue:StringEquals": {
	"aws:PrincipalTag/RedshiftDbUser": "dbUser"
	}	

환경 유형	IAM 권한	

```
      }
    },
    {
      "Sid": "VisualEd
itor2",
      "Effect": "Allow",
      "Action": [
        "redshift-
data:DescribeStat
ement",
        "redshift-
data:ExecuteStatement"
      ],
      "Resource":
 "arn:aws:redshift:
region:account-id:
cluster:cluster-id
entifier"
    }
  ]
}
```

환경 유형	IAM 권한	

Amazon Redshift 쿼리 편집기 v2	{
	"Version": "2012-10-17",
	"Statement": [
	{
	"Action": "redshift:DescribeClusters",
	"Effect": "Allow",
	"Resource": "arn:aws:redshift:region:account-id:cluster:*",
	"Sid": "RedshiftPermissions"
	},
	{
	"Action": "tag:GetResources",
	"Condition": {
	"StringEquals": { "aws:CalledViaLast": "sqlworkbench.amazonaws.com" }
	},
	"Effect": "Allow",
	"Resource": "*",
	"Sid": "ResourceGroupsTaggingPermissions"
	},
	{
	"Action": [
	"sqlworkbench:DriverExecute",
	"sqlworkbench:GenerateSession",	

환경 유형	IAM 권한	

```
        "sqlworkb
ench:ListConnectio
ns",
        "sqlworkb
ench:ListDatabases",
        "sqlworkb
ench:ListFiles",
        "sqlworkb
ench:ListNotebooks",
        "sqlworkb
ench:ListQueryExec
utionHistory",
        "sqlworkb
ench:ListRedshiftC
lusters",
        "sqlworkb
ench:ListSampleDat
abases",
        "sqlworkb
ench:ListTabs",
        "sqlworkb
ench:ListTaggedRes
ources"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Sid": "AmazonRe
dshiftQueryEditorV
2PermissionsPart1"
    },
    {
      "Action":
 "sqlworkbench:*",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:
sqlworkbench:regio
n:account-id:query/
*",
        "arn:aws:
sqlworkbench:regio
```

환경 유형	IAM 권한	

```
n:account-id:noteb
ook/*",
        "arn:aws:
sqlworkbench:regio
n:account-id:conne
ction/*",
        "arn:aws:
sqlworkbench:regio
n:account-id:chart/
*",
        "arn:aws:
sqlworkbench:regio
n:account-id:/*"
      ],
      "Sid": "AmazonRe
dshiftQueryEditorV
2PermissionsPart2"
    }
  ]
}
```

임시 자격 증명

임시 자격 증명을 사용하여 로그인하면 일부 AWS 서비스가 작동하지 않습니다. 임시 자격 증명으로 작동하는 AWS 서비스를 비롯한 추가 정보는 IAM 사용 설명서의 IAM과 호환되는AWS 서비스를 참조하십시오.

사용자 이름과 암호를 제외한 다른 방법을 AWS Management Console 사용하여 로그인하면 임시 자격 증명을 사용하는 것입니다. 예를 들어 회사의 SSO (Single Sign-On) 링크를 AWS 사용하여 액세스하는 경우 이 프로세스에서 자동으로 임시 자격 증명을 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 보안 인증을 자동으로 생성합니다. 역할 전환에 대한 자세한 정보는 IAM 사용 설명서의 역할로 전환(콘솔)을 참조하세요.

또는 API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다 AWS CLI . AWS 그런 다음 해당 임시 자격 증명을 사용하여 액세스할 수 AWS있습니다. AWS 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성할 것을 권장합니다. 자세한 정보는 IAM의 임시 보안 인증 섹션을 참조하세요.

보안 주체 권한

IAM 사용자 또는 역할을 사용하여 작업을 수행하는 AWS경우 보안 주체로 간주됩니다. 정책은 보안 주체에게 권한을 부여합니다. 일부 서비스를 사용할 때는 다른 서비스에서 다른 작업을 트리거하는 작업을 수행할 수 있습니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. 작업에 따라 정책에서 종속 작업이 추가로 필요한지 여부를 알아보려면 서비스 권한 부여 참조의 AWS 문서 필수 항목에 대한 작업, 리소스 및 조건 키를 참조하십시오.

Amazon에 대한 규정 준수 검증 DataZone

특정 규정 준수 프로그램의 범위 내에 AWS 서비스 있는지 알아보려면AWS 서비스 규정 준수 프로그램의AWS 서비스 범위별, 규정 참조하여 관심 있는 규정 준수 프로그램을 선택하십시오. 일반 정보는 AWS 규정 준수 프로그램AWS 보증 프로그램 규정AWS 참조하십시오.

를 사용하여 AWS Artifact타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 의 보고서 https://docs.aws.amazon.com/artifact/latest/ug/downloading-documents.html 참조하십시오 AWS Artifact.

사용 시 규정 준수 AWS 서비스 책임은 데이터의 민감도, 회사의 규정 준수 목표, 관련 법률 및 규정에 따라 결정됩니다. AWS 규정 준수에 도움이 되는 다음 리소스를 제공합니다.

- 보안 및 규정 준수 퀵 스타트 가이드 - 이 배포 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수에 AWS 중점을 둔 기본 환경을 배포하기 위한 단계를 제공합니다.
- Amazon Web Services의 HIPAA 보안 및 규정 준수를 위한 설계 — 이 백서에서는 기업이 HIPAA 적격 애플리케이션을 만드는 AWS 데 사용할 수 있는 방법을 설명합니다.

> **Note**
>
> 모든 AWS 서비스 사람이 HIPAA 자격을 갖춘 것은 아닙니다. 자세한 내용은 HIPAA 적격 서비스 참조를 참조하십시오.

- AWS 규정 준수 리소스AWS — 이 워크북 및 가이드 모음은 해당 산업 및 지역에 적용될 수 있습니다.
- AWS 고객 규정 준수 가이드 — 규정 준수의 관점에서 공동 책임 모델을 이해하십시오. 이 가이드에서는 보안을 유지하기 위한 모범 사례를 AWS 서비스 요약하고 여러 프레임워크 (미국 표준 기술 연구소 (NIST), 결제 카드 산업 보안 표준 위원회 (PCI), 국제 표준화기구 (ISO) 등) 에서 보안 제어에 대한 지침을 매핑합니다.

- AWS Config 개발자 안내서의 규칙을 사용하여 리소스 평가 — 이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub— 이를 AWS 서비스 통해 내부 AWS보안 상태를 포괄적으로 파악할 수 있습니다. Security Hub는 보안 제어를 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하십시오.
- Amazon GuardDuty — 환경에 의심스럽고 악의적인 활동이 있는지 AWS 계정모니터링하여 워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 AWS 서비스 탐지합니다. GuardDuty 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하여 PCI DSS와 같은 다양한 규정 준수 요구 사항을 해결하는 데 도움이 될 수 있습니다.
- AWS Audit Manager— 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위험을 관리하고 규정 및 업계 표준을 준수하는 방법을 단순화할 수 있습니다.

Amazon의 보안 모범 사례 DataZone

DataZone Amazon은 자체 보안 정책을 개발하고 구현할 때 고려해야 할 여러 보안 기능을 제공합니다. 다음 모범 사례는 일반적인 지침이며 완벽한 보안 솔루션을 나타내지는 않습니다. 이러한 모범 사례는 환경에 적절하지 않거나 충분하지 않을 수 있으므로 참고용으로만 사용해 주세요.

최소 권한 액세스 구현

권한을 부여할 때는 누가 어떤 Amazon DataZone 리소스에 어떤 권한을 부여할지 결정합니다. 해당 리소스에서 허용할 작업을 사용 설정합니다. 따라서 작업을 수행하는 데 필요한 권한만 부여해야 합니다. 최소 권한 액세스를 구현하는 것이 오류 또는 악의적인 의도로 인해 발생할 수 있는 보안 위험과 영향을 최소화할 수 있는 근본적인 방법입니다.

IAM 역할 사용

생산자 및 클라이언트 애플리케이션이 Amazon DataZone 리소스에 액세스하려면 유효한 자격 증명이 있어야 합니다. AWS 자격 증명을 클라이언트 애플리케이션이나 Amazon S3 버킷에 직접 저장해서는 안 됩니다. 이러한 보안 인증은 자동으로 교체되지 않으며 손상된 경우 비즈니스에 큰 영향을 줄 수 있는 장기 보안 인증입니다.

대신 IAM 역할을 사용하여 생산자 및 클라이언트 애플리케이션이 Amazon DataZone 리소스에 액세스할 수 있도록 하기 위한 임시 자격 증명을 관리해야 합니다. 역할을 사용하면 장기 자격 증명(예: 사용자 이름과 암호 또는 액세스 키)을 사용하여 다른 리소스에 액세스할 필요가 없습니다.

자세한 설명은 IAM 사용자 가이드에서 다음 주제를 참조하십시오:

- IAM 역할
- 역할에 대한 일반적인 시나리오: 사용자, 애플리케이션 및 서비스

종속 리소스에서 서버 측 암호화 구현

Amazon에서는 저장된 데이터와 전송 중인 데이터를 암호화할 수 DataZone 있습니다.

API 호출을 모니터링하는 CloudTrail 데 사용합니다.

DataZone Amazon은 Amazon에서 사용자 AWS CloudTrail, 역할 또는 서비스가 수행한 작업의 기록을 제공하는 AWS 서비스와 통합되어 DataZone 있습니다.

에서 수집한 CloudTrail 정보를 사용하여 Amazon에 요청한 내용 DataZone, 요청한 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다.

아마존의 레질리언스 DataZone

AWS 글로벌 인프라는 가용 영역을 중심으로 구축됩니다 AWS 리전 . AWS 리전 물리적으로 분리되고 격리된 여러 가용 영역을 제공합니다. 이 가용 영역은 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워킹으로 연결됩니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 극복 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

가용 영역에 대한 AWS 리전 자세한 내용은 글로벌 인프라를 참조하십시오AWS .

AWS 글로벌 인프라 외에도 DataZone Amazon은 데이터 복원력 및 백업 요구 사항을 지원하는 데 도움이 되는 여러 기능을 제공합니다.

주제

- 데이터 소스 복원력
- 자산 레질리언스
- 에셋 유형과 메타데이터는 복원력을 형성합니다.
- 용어집 복원력
- 글로벌 검색 복원력
- 서브스크립션 레질리언스
- 환경 복원력
- 환경 블루프린트 레질리언스

- 프로젝트 레질리언스
- RAM 복원력
- 사용자 프로필 관리 레질리언스
- 도메인 레질리언스

데이터 소스 복원력

Amazon DataZone 가용성 이벤트 중에는 `DataSource` 작업이 최대 24시간 동안 주기적으로 재시도됩니다. 잘못된 구성으로 인해 작업이 실패하는 경우 `DataSourceRunFailed` 이벤트가 발생합니다. Amazon DataZone 도메인이 KMS 키로 구성되어 있는데 작업 실행 중에 이 키에 액세스할 수 없는 경우 해당 `INACCESSIBLE` 상태에서 실행이 종료됩니다. AmazonDataZoneDomainExecutionRole KMS 액세스가 복원되면 작업을 수동으로 업데이트하여 사용 가능한 상태로 다시 전환하도록 트리거해야 합니다.

자산 레질리언스

DataZoneAmazon에서는 자산에 버전이 지정됩니다. 자산 버전을 롤백해야 하는 경우 가장 최근의 안정 버전의 콘텐츠를 사용하여 새 버전을 생성할 수 있습니다. 자산 버전을 게시할 수 있습니다. 게시된 버전의 자산은 새 버전을 게시하는 경우를 제외하고는 편집할 수 없습니다. 게시된 자산 (일명 목록) 을 구독할 수 있습니다. 자산에 대한 신규 구독을 방지하기 위해 게시를 취소할 수 있습니다. 자산 게시를 취소해도 기존 구독에는 영향을 미치지 않습니다. 자산을 삭제하면 게시되지 않은 버전의 자산이 모두 삭제됩니다. 게시된 버전의 에셋은 별도로 삭제해야 합니다. 구독이 없는 경우에만 게시된 버전의 자산을 삭제할 수 있습니다.

에셋 유형과 메타데이터는 복원력을 형성합니다.

DataZoneAmazon에서는 자산 유형과 메타데이터 양식 유형에 버전이 지정됩니다. 자산에서 사용 중인 자산 유형은 삭제할 수 없습니다. 자산 유형이나 자산에서 사용 중인 메타데이터 양식 유형은 삭제할 수 없습니다. 큐레이션에 특정 metadata-form-type 항목을 사용하지 않으려면 이미 첨부된 항목에는 영향을 주지 않도록 설정할 수 있습니다. 이렇게 하면 해당 항목이 이미 첨부된 항목에는 영향을 주지 않습니다.

용어집 복원력

DataZoneAmazon에서 용어집 및 용어집 용어는 사용 중인 경우 삭제할 수 없습니다. 특정 용어집이나 용어를 큐레이션에 사용하지 않으려면 해당 용어집이나 용어집을 비활성화할 수 있습니다. 이렇게 하면 이미 첨부된 용어집에는 영향을 주지 않습니다.

글로벌 검색 복원력

DataZoneAmazon에서는 글로벌 검색을 통해 게시된 자산 (일명 리스팅) 을 검색할 수 있습니다. 자산 게시를 취소하여 자산 게시를 롤백할 수 있습니다. 자산 게시를 취소해도 기존 구독에는 영향을 주지 않습니다. 게시된 자산을 해당 버전을 다시 게시하여 해당 버전의 자산으로 롤백할 수 있습니다. 기존 구독에는 영향을 주지 않습니다.

서브스크립션 레질리언스

DataZoneAmazon에서는 SubscriptionGrant 주문 처리가 실패하기 전에 두 번 사용 중단을 시도합니다. 실패할 경우 다시 시도하려면 수동으로 삭제해야 합니다. Amazon이 구독 권한을 DataZone 취소할 수 없는 경우 구독 삭제가 실패할 수 있습니다. 근본적인 오류를 해결하거나 `DeleteSubscriptionGrant` API 작업에서 `retainPermissions` 플래그를 사용하여 권한을 DataZone 취소하지 않고 Amazon에서 권한 부여를 강제로 삭제할 수 있습니다.

Amazon DataZone 도메인이 KMS 키로 구성되어 있는데 `SubscriptionGrant` 워크플로 중에 이 키에 대한 액세스 권한을 `AmazonDataZoneDomainExecutionRole` 잃으면 권한이 표시됩니다`INACCESSIBLE`. KMS 액세스가 복원되면 권한 `INACCESSIBLE` 부여를 삭제하고 다시 생성해야 합니다.

환경 복원력

Amazon DataZone 도메인이 KMS 키로 구성되어 있는데 환경 워크플로 중에 이 키에 액세스할 수 없는 경우 환경이 표시됩니다`INACCESSIBLE`. `AmazonDataZoneDomainExecutionRole` KMS 액세스를 복원한 후에는 `INACCESSIBLE` 환경을 삭제하고 다시 만들어야 합니다. 환경 생성은 실패하기 전에 중단을 두 번 시도합니다. 실패할 경우 다시 시도하려면 수동으로 삭제해야 합니다. 환경 워크플로가 실패하면 환경은 실패 상태가 됩니다. 지금은 삭제하고 다시 만들 수만 있습니다.

환경 블루프린트 레질리언스

DataZoneAmazon에서는 기본 환경 프로필이 있는 경우 환경 청사진을 삭제할 수 없습니다.

프로젝트 레질리언스

DataZoneAmazon에서는 포함된 환경이 있는 경우 프로젝트를 삭제할 수 없습니다.

RAM 복원력

RAM 레질리언스 정보는 https://docs.aws.amazon.com/ram/latest/userguide/ security-disaster-recovery-resiliency .html을 참조하십시오.

사용자 프로필 관리 레질리언스

사용자 프로필 복원 정보는 AWS Identity Center를 참조하십시오.

도메인 레질리언스

DataZoneAmazon에서는 프로젝트 또는 데이터 소스가 포함된 도메인을 삭제할 수 없습니다.

아마존의 인프라 보안 DataZone

DataZone Amazon은 관리형 서비스로서 AWS 글로벌 네트워크 보안의 보호를 받습니다. AWS 보안 서비스 및 인프라 AWS 보호 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하십시오. 인프라 보안 모범 사례를 사용하여 AWS 환경을 설계하려면 Security Pillar AWS Well-Architected Framework의 인프라 보호를 참조하십시오.

AWS 게시된 API 호출을 사용하여 네트워크를 DataZone 통해 Amazon에 액세스합니다. 고객은 다음을 지원해야 합니다.

- 전송 계층 보안(TLS) TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군 Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 요청은 액세스 키 ID 및 IAM 주체와 관련된 비밀 액세스 키를 사용하여 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 보안 인증을 생성하여 요청에 서명할 수 있습니다.

Amazon의 서비스 간 혼란을 야기한 대리인 예방 DataZone

혼동된 대리자 문제는 작업을 수행할 권한이 없는 엔터티가 권한이 더 많은 엔터티에게 작업을 수행하도록 강요할 수 있는 보안 문제입니다. 에서 AWS, 서비스 간 사칭은 대리인 혼동을 야기할 수 있습니다. 교차 서비스 가장은 한 서비스(직접 호출하는 서비스)가 다른 서비스(직접 호출되는 서비스)를 직접 호출할 때 발생할 수 있습니다. 직접 호출하는 서비스는 다른 고객의 리소스에 대해 액세스 권한이 없는 방식으로 작동하게 권한을 사용하도록 조작될 수 있습니다. 이를 방지하기 위해 계정 내 리소스에 대한 액세스 권한이 부여된 서비스 보안 주체를 통해 모든 서비스의 데이터를 보호하는 데 도움이 되는 도구를 AWS 제공합니다.

Amazon이 다른 서비스에 리소스에 DataZone 부여하는 권한을 제한하려면 리소스 정책에 aws:SourceAccount 글로벌 조건 컨텍스트 키를 사용하는 것이 좋습니다. SourceAccount 해당 계정의 모든 리소스가 교차 서비스 사용과 연결되도록 허용하려면 aws를 사용하십시오.

Amazon의 구성 및 취약성 분석 DataZone

AWS 게스트 운영 체제 (OS) 및 데이터베이스 패치, 방화벽 구성, 재해 복구와 같은 기본 보안 작업을 처리합니다. 적합한 제3자가 이 절차를 검토하고 인증하였습니다. 자세한 내용은 AWS 공동 책임 모델을 참조하십시오.

허용 목록에 추가할 도메인

Amazon DataZone 데이터 포털이 Amazon DataZone 서비스에 액세스하려면 데이터 포털이 서비스에 액세스하려는 네트워크의 허용 목록에 다음 도메인을 추가해야 합니다.

- `*.api.aws`
- `*.on.aws`

아마존 모니터링 DataZone

모니터링은 Amazon 및 기타 AWS 솔루션의 안정성, 가용성 및 성능을 유지하는 데 DataZone 있어 중요한 부분입니다. AWS 는 Amazon을 감시하고, 문제 발생 시 보고하고 DataZone, 적절한 경우 자동 조치를 취할 수 있는 다음과 같은 모니터링 도구를 제공합니다.

- Amazon은 실행 중인 AWS 리소스와 애플리케이션을 AWS 실시간으로 CloudWatch 모니터링합니다. 지표를 수집 및 추적하고, 맞춤 대시보드를 생성할 수 있으며, 지정된 지표가 지정한 임계값에 도달하면 사용자에게 알리거나 조치를 취하도록 경보를 설정할 수 있습니다. 예를 들어 Amazon EC2 인스턴스의 CPU 사용량 또는 기타 지표를 CloudWatch 추적하고 필요할 때 새 인스턴스를 자동으로 시작할 수 있습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하십시오.
- Amazon CloudWatch Logs를 사용하면 Amazon EC2 인스턴스 및 기타 소스에서 로그 파일을 모니터링 CloudTrail, 저장 및 액세스할 수 있습니다. CloudWatch 로그는 로그 파일의 정보를 모니터링하고 특정 임계값이 충족되면 알려줄 수 있습니다. 또한 매우 내구력 있는 스토리지에 로그 데이터를 저장할 수 있습니다. 자세한 내용은 Amazon CloudWatch Logs 사용 설명서를 참조하십시오.
- Amazon을 사용하면 AWS 서비스를 자동화하고 애플리케이션 가용성 문제 또는 리소스 변경과 같은 시스템 이벤트에 자동으로 대응할 EventBridge 수 있습니다. AWS 서비스에서 발생하는 이벤트는 거의 EventBridge 실시간으로 전송됩니다. 원하는 이벤트만 표시하도록 간단한 규칙을 작성한 후 규칙과 일치하는 이벤트 발생 시 실행할 자동화 작업을 지정할 수 있습니다. 자세한 내용은 Amazon EventBridge 사용 설명서를 참조하십시오.
- AWS CloudTrail계정에서 또는 AWS 계정을 대신하여 이루어진 API 호출 및 관련 이벤트를 캡처하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 어떤 사용자와 계정이 전화를 걸었는지 AWS, 어떤 소스 IP 주소에서 호출이 이루어졌는지, 언제 호출이 발생했는지 식별할 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

아마존을 DataZone 통한 아마존 모니터링 CloudWatch

원시 데이터를 수집하여 읽기 쉬운 거의 실시간 지표로 처리하는 DataZone 를 사용하여 CloudWatch Amazon을 모니터링할 수 있습니다. 이러한 통계는 15개월간 보관되므로 기록 정보에 액세스하고 웹 애플리케이션 또는 서비스가 어떻게 실행되고 있는지 전체적으로 더 잘 파악할 수 있습니다. 특정 임계값을 주시하다가 해당 임계값이 충족될 때 알림을 전송하거나 조치를 취하도록 경보를 설정할 수도 있습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하십시오.

Amazon DataZone 데이터 포털은 JWT 인증 및 권한 부여와 함께 Amazon DataZone 데이터 플레인 API를 사용합니다. DataZone Amazon은 Amazon DataZone 기본 서비스 역할을

맡고 Amazon DataZone 데이터 포털을 통해 이루어진 모든 Amazon DataZone API 호출을 DataZoneDataPortalCallLogsAPI라는 로그 그룹에 기록합니다.

아마존에서 아마존 DataZone 이벤트 모니터링 EventBridge

자체 애플리케이션 EventBridge, software-as-a-service (SaaS) 애플리케이션 및 AWS 서비스로부터 실시간 데이터 스트림을 제공하는 Amazon DataZone 이벤트를 모니터링할 수 있습니다. EventBridge 해당 데이터를 Amazon 심플 알림 AWS Lambda 서비스와 같은 대상으로 라우팅합니다. 이러한 이벤트는 AWS 리소스 변경을 설명하는 시스템 CloudWatch 이벤트의 스트림을 거의 실시간으로 제공하는 Amazon Events에 나타나는 이벤트와 동일합니다.

자세한 내용은 Amazon EventBridge 기본 버스를 통한 이벤트 처리을(를) 참조하세요.

를 사용하여 Amazon DataZone API 호출을 로깅합니다. AWS CloudTrail

DataZone Amazon은 Amazon에서 사용자 AWS CloudTrail, 역할 또는 서비스가 수행한 작업의 기록을 제공하는 AWS 서비스와 통합되어 DataZone 있습니다. CloudTrail Amazon에 대한 모든 API 호출을 DataZone 이벤트로 캡처합니다. 캡처된 호출에는 Amazon DataZone 콘솔에서의 호출 및 Amazon DataZone API 작업에 대한 코드 호출이 포함됩니다. 트레일을 생성하면 Amazon 이벤트를 포함하여 Amazon S3 버킷으로 CloudTrail 이벤트를 지속적으로 전송할 수 DataZone 있습니다. 트레일을 구성하지 않아도 CloudTrail 콘솔의 이벤트 기록에서 가장 최근 이벤트를 계속 볼 수 있습니다. 에서 수집한 CloudTrail 정보를 사용하여 Amazon에 요청한 내용 DataZone, 요청한 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다.

자세한 CloudTrail 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

아마존 DataZone 정보 입력 CloudTrail

CloudTrail 계정을 만들 AWS 계정 때 활성화됩니다. Amazon DataZone 관리 콘솔에서 활동이 발생하면 해당 활동이 CloudTrail 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 이벤트에 기록됩니다. 내 사이트에서 최근 이벤트를 보고, 검색하고, 다운로드할 수 있습니다 AWS 계정. 자세한 내용은 이벤트 기록으로 CloudTrail 이벤트 보기를 참조하십시오.

DataZoneAmazon의 이벤트를 포함하여 귀하의 이벤트에 대한 지속적인 기록을 AWS 계정보려면 트레일을 생성하십시오. 트레일을 사용하면 CloudTrail Amazon S3 버킷에 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 트레일은 AWS 파

티션에 있는 모든 지역의 이벤트를 기록하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 이에 따라 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음을 참조하십시오.

- 추적 생성 개요
- CloudTrail 지원되는 서비스 및 통합
- 에 대한 Amazon SNS 알림 구성 CloudTrail
- 여러 지역에서 CloudTrail 로그 파일 수신 및 여러 계정으로부터 CloudTrail 로그 파일 수신

모든 Amazon DataZone 작업은 로그에 의해 기록됩니다 CloudTrail.

아마존 문제 해결 DataZone

Amazon에서 작업할 때 액세스 거부 문제 또는 유사한 문제가 발생하는 경우 이 DataZone 섹션의 주제를 참조하십시오.

Amazon의 AWS Lake Formation 권한 문제 해결 DataZone

이 섹션에는 다음과 같은 경우에 발생할 수 있는 문제에 대한 문제 해결 지침이 포함되어 Amazon에 대한 Lake Formation 권한 구성 DataZone 있습니다.

데이터 포털의 오류 메시지	해결 방법
데이터 액세스 역할을 맡을 수 없습니다.	이 오류는 DefaultDataLakeBlueprint계정에서 활성화하는 데 사용한 내용을 DataZone Amazon에서 추정할 수 없을 때 표시됩니다. AmazonDataZoneGlueDataAccessRole 문제를 해결하려면 데이터 자산이 있는 계정의 AWS IAM 콘솔로 이동하여 Amazon DataZone 서비스 보안 주체와 올바른 신뢰 관계를 맺고 있는지 확인하십시오. AmazonDataZoneGlue DataAccessRole 자세한 내용은 AmazonDataZoneGlueAccess- <region>- <domainId>단원을 참조하세요.
데이터 액세스 역할에는 구독하려는 자산의 메타데이터를 읽는 데 필요한 권한이 없습니다.	Amazon이 역할을 DataZone 성공적으로 수임했지만 AmazonDataZoneGlueDataAccessRole역할에 필요한 권한이 없는 경우 이 오류가 표시됩니다. 문제를 해결하려면 데이터 자산이 있는 계정의 AWS IAM 콘솔로 이동하여 역할에 데이터 자산이 AmazonDataZoneGlueManageAccessRolePolicy연결되어 있는지 확인하십시오. 자세한 정보는 AmazonDataZoneGlueAccess- <region>- <domainId>을 참조하세요.

데이터 포털의 오류 메시지	해결 방법
에셋은 리소스 링크입니다. DataZone Amazon은 리소스 링크 구독을 지원하지 않습니다.	Amazon에 게시하려는 자산이 AWS Glue 테이블에 대한 리소스 링크인 경우 DataZone 이 오류가 표시됩니다.
자산은 AWS Lake Formation에서 관리하지 않습니다.	이 오류는 게시하려는 자산에 AWS Lake Formation 권한이 적용되지 않았음을 나타냅니다. 이는 다음과 같은 경우에 발생할 수 있습니다. • 자산의 Amazon S3 위치는 AWS Lake Formation에 등록되어 있지 않습니다. 문제를 해결하려면 테이블이 있는 계정으로 AWS Lake Formation 콘솔에 로그인하고 AWS Lake Formation 모드 또는 하이브리드 모드에서 Amazon S3 위치를 등록하십시오. 자세한 내용을 알아보려면 Registering an Amazon S3 location(Amazon S3 위치 등록)을 참조하세요. 추가 수정이 필요한 몇 가지 시나리오가 있습니다. 여기에는 암호화된 AmazonS3 버킷 또는 계정 간 S3 버킷 및 Glue AWS 카탈로그 설정이 포함됩니다. 이러한 경우 KMS 및/또는 S3 설정을 수정해야 할 수 있습니다. 자세한 내용을 알아보려면 암호화된 Amazon S3 위치 등록을 참조하십시오. • Amazon S3 위치는 AWS Lake Formation 모드에서 등록되지만 테이블 권한에 AllowedPrincipalIAM이 추가됩니다. 문제를 해결하려면 테이블 AllowedPrincipal 권한에서 IAM을 제거하거나 하이브리드 모드에서 S3 위치를 등록하면 됩니다. 자세한 내용은 Lake Formation 권한 모델로의 업그레이드 정보를 참조하십시오. S3 위치가 암호화되어 있거나 S3 위치가 AWS Glue 테이블과 다른 계정에 있는 경우 암호화된 Amazon S3 위치 등록의 지침을 따르십시오.

데이터 포털의 오류 메시지	해결 방법
데이터 액세스 역할에는 이 자산에 대한 액세스 권한을 부여하는 데 필요한 Lake Formation 권한이 없습니다.	이 오류는 DefaultDataLakeBlueprint계정에서 AmazonDataZoneGlueDataAccessRole활성화하는 데 사용하는 항목에 Amazon이 게시된 자산에 대한 권한을 관리하는 DataZone 데 필요한 권한이 없음을 나타냅니다. 을 (를) AWS Lake Formation 관리자로 추가하거나 게시하려는 AmazonDataZoneGlueDataAccessRole자산에 다음 권한을 부여하여 문제를 해결할 수 있습니다. AmazonDataZoneGlueDataAccessRole • 자산이 있는 데이터베이스에 부여할 수 있는 권한을 설명하고 설명하십시오. • DataZone Amazon이 사용자를 대신하여 관리하기를 원하는 데이터베이스의 모든 자산에 대한 액세스 권한을 설명, 선택, 허용 가능으로 설명, 부여 가능 여부를 선택합니다.

아마존 할당량 DataZone

AWS 계정에는 각 서비스에 대한 기본 할당량 (이전에는 한도라고 함) 이 있습니다. AWS 다르게 표시되지 않는 한, 리전별로 각 할당량이 적용됩니다.

DataZone Amazon에는 다음과 같은 할당량 및 한도가 있습니다.

Resource	설명	값
데이터 자산 유형	DataZone 도메인에서 생성할 수 있는 최대 데이터 자산 유형 수	1000
데이터 자산	Amazon DataZone 도메인에서 생성할 수 있는 최대 데이터 자산 수	100만
용어집	도메인에서 만들 수 있는 비즈니스 용어집의 최대 개수	1000
비즈니스 용어집 용어	도메인에서 만들 수 있는 총 비즈니스 용어집 용어의 최대 수	10000
도메인 내 환경	Amazon DataZone 도메인의 최대 환경 수	500

Amazon DataZone 사용 설명서의 문서 기록

다음 표에는 Amazon의 설명서 릴리스가 설명되어 DataZone 있습니다.

변경 사항	설명	날짜
AmazonDataZoneSageMakerProvisioning - 새 정책	Amazon이라는 새 정책은 DataZone Amazon과 상호 운용하는 데 필요한 권한을 SageMaker Amazon에 AmazonDataZoneSageMakerProvisioning부여합니다. 자세한 내용은 AWS 관리형 정책에 대한 Amazon DataZone 업데이트를 참조하십시오.	2024년 4월 30일
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary - 새 권한 경계	새 권한 경계가 AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary호출되었습니다. Amazon DataZone 데이터 포털을 통해 Amazon SageMaker 환경을 생성하면 Amazon은 환경 생성 중에 생성되는 IAM 역할에 이 권한 경계를 DataZone 적용합니다. 권한 경계는 Amazon이 DataZone 생성하는 역할 및 사용자가 추가하는 모든 역할의 범위를 제한합니다. 자세한 내용은 AWS 관리형 정책에 대한 Amazon DataZone 업데이트를 참조하십시오.	2024년 4월 30일
AmazonDataZoneSageMakerAccess - 새 정책	라는 AmazonDataZoneSageMakerAccess새 정책은 Amazon DataZone SageMaker	2024년 4월 30일

	환경의 다양한 리소스에 대한 사용자 액세스 권한을 부여하는 데 필요한 권한을 Amazon에 부여합니다. 자세한 내용은 AWS 관리형 정책에 대한 Amazon DataZone 업데이트를 참조하십시오.	
AmazonDataZoneFullAccess - 정책 업데이트	콘솔에서 블루프린트를 구성하고 지정된 관리형 AmazonDataZoneFullAccess정책에 대한 정보를 검색하는 데 도움이 되는 `DescribeSecurityGroups` 작업을 구성하는 계정 관리자의 편의성을 개선하기 위해 `GetPolicy` 작업에 대한 액세스 권한을 추가하는 정책 업데이트입니다. 자세한 내용은 AWS 관리형 정책에 대한 Amazon DataZone 업데이트를 참조하십시오.	2024년 4월 30일
AmazonDataZoneS3Manage- - - 새 역할 <region><domainId>	AmazonDataZoneS3Manage-라는 새로운 역할 - <region><domainId>아마존이 AWS Lake Formation을 DataZone 호출하여 아마존 심플 스토리지 서비스 (Amazon S3) 의 위치를 등록할 때 사용됩니다. AWS Lake Formation은 해당 위치의 데이터에 액세스할 때 이 역할을 맡습니다. 자세한 내용은 AWS 관리형 정책에 대한 Amazon DataZone 업데이트를 참조하십시오.	2024년 4월 1일

AmazonDataZoneGlueManageAccessRolePolicy - 정책 업데이트	Amazon이 AmazonDataZoneGlueManageAccessRolePolicy데이터에 대한 게시 및 액세스 권한 DataZone 부여를 활성화할 수 있는 권한에 대한 지원을 활성화하도록 업데이트되었습니다. 자세한 내용은 AWS 관리형 정책에 대한 Amazon DataZone 업데이트를 참조하십시오.	2024년 4월 1일
AmazonDataZoneDomainExecutionRolePolicy 및 AmazonDataZoneFullUserAccess - 정책 업데이트	`CancelMetadataGenerationRun` API에 대한 지원을 AmazonDataZoneFullUserAccess활성화하도록 AmazonDataZoneDomainExecutionRolePolicy및 를 업데이트했습니다. 자세한 내용은 AWS 관리형 정책에 대한 Amazon DataZone 업데이트를 참조하십시오.	2024년 3월 29일
AmazonDataZoneFullAccess - 정책 업데이트	사용자가 텍스트 상자에 입력하지 않고 Amazon DataZone 관리 콘솔에서 암호, 클러스터, vpc 및 서브넷을 선택할 수 있도록 업데이트되었습니다. `AmazonDataZoneFullAccess` 자세한 내용은 AWS 관리형 정책에 대한 Amazon DataZone 업데이트를 참조하십시오.	2024년 3월 13일

AmazonDataZoneDomainExecutionRolePolicy - 정책 업데이트	어떤 계정과 지역에서 어떤 블루프린트가 활성화되었는지 식별하여 환경 프로필 생성에 필요한 ListEnvironmentBlueprintConfigurationSummaries API를 지원할 수 있도록 업데이트되었습니다. AmazonDataZoneDomainExecutionRolePolicy 자세한 내용은 AWS 관리형 정책에 대한 Amazon DataZone 업데이트를 참조하십시오.	2024년 2월 1일
AmazonDataZoneGlueManageAccessRolePolicy - 정책 업데이트	AWS Lake Formation 하이브리드 모드를 지원할 수 AmazonDataZoneGlueManageAccessRolePolicy있도록 업데이트되었습니다. 자세한 내용은 AWS 관리형 정책에 대한 Amazon DataZone 업데이트를 참조하십시오.	2023년 12월 14일
AmazonDataZoneFullUserAccess 및 AmazonDataZoneDomainExecutionRolePolicy - 정책 업데이트	Amazon은 Amazon의 생성적 AI 기반 데이터 설명 기능을 지원하도록 AmazonDataZoneFullUserAccess및 AmazonDataZoneDomainExecutionRolePolicy정책을 DataZone 업데이트했습니다. DataZone 자세한 내용은 AWS 관리형 정책에 대한 Amazon DataZone 업데이트를 참조하십시오.	2023년 11월 28일

AmazonDataZoneEnvironmentRolePermissionsBoundary - 정책 업데이트	DataZone Amazon은 `ResourceTag` 조건에 따라 범위가 축소된 추가 `athena:GetQueryResultsStream` 권한으로 구성된 AmazonDataZoneEnvironmentRolePermissionsBoundary관리형 정책을 업데이트했습니다. 자세한 내용은 AWS 관리형 정책에 대한 Amazon DataZone 업데이트를 참조하십시오.	2023년 11월 17일
AmazonDataZoneRedshiftManageAccessRolePolicy - 정책 업데이트	Amazon은 해당 `redshift:AssociateDataShareConsumer` 작업에 대한 조직 ID 확인을 제거하여 AmazonDataZoneRedshiftManageAccessRolePolicy정책을 DataZone 업데이트했습니다. 이렇게 하면 AWS 조직 간에 리소스를 공유할 수 있습니다. 자세한 내용은 AWS 관리형 정책에 대한 Amazon DataZone 업데이트를 참조하십시오.	2023년 11월 16일

AmazonDataZoneFull UserAccess - 정책 업데이트	Amazon은 DataZone Amazon에 대한 전체 액세스 권한을 부여하는 AmazonDataZoneFull UserAccess정책을 DataZone 업데이트했지만 도메인, 사용자 또는 관련 계정의 관리는 허용하지 않습니다. 자세한 내용은 AWS 관리형 정책에 대한 Amazon DataZone 업데이트를 참조하십시오.	2023년 10월 2일
AmazonDataZonePrev iewConsoleFullAccess - 정책은 더 이상 사용되지 않습니다.	Amazon은 더 DataZone 이상 사용되지 않습니다 AmazonDataZonePrev iewConsoleFullAccess. 자세한 내용은 관리형 정책에 대한 Amazon DataZone 업데이트를 참조하십시오. AWS	2023년 9월 29일
AmazonDataZonePort alFullAccessPolicy - 정책은 더 이상 사용되지 않습니다.	Amazon은 더 DataZone 이상 사용되지 않습니다 AmazonDataZonePort alFullAccessPolicy. 자세한 내용은 관리형 정책에 대한 Amazon DataZone 업데이트를 참조하십시오. AWS	2023년 9월 29일

AmazonDataZoneDomainExecutionRolePolicy - 새 정책	Amazon은 이라는 새 정책을 DataZone 추가했습니다 AmazonDataZoneDomainExecutionRolePolicy. Amazon DataZone `AmazonDataZoneDomainExecutionRole` 서비스 역할의 기본 정책입니다. Amazon은 이 역할을 DataZone 사용하여 Amazon DataZone 도메인의 데이터를 카탈로그, 검색, 관리, 공유 및 분석합니다. 정책을 귀하의 `AmazonDataZoneDomainExecutionRolePolicy` `AmazonDataZoneDomainExecutionRole` 정책에 첨부할 수 있습니다. 자세한 내용은 AWS 관리형 정책에 대한 Amazon DataZone 업데이트를 참조하십시오.	2023년 9월 25일
AmazonDataZoneCrossAccountAdmin - 새 정책	Amazon은 사용자가 Amazon DataZone 및 관련 계정을 사용할 수 있도록 하는 새로운 정책을 DataZone 추가했습니다. AmazonDataZoneCrossAccountAdmin 자세한 내용은 AWS 관리형 정책에 대한 Amazon DataZone 업데이트를 참조하십시오.	2023년 9월 19일

AmazonDataZoneRedshiftManageAccessRolePolicy - 새 정책	Amazon은 AmazonDataZoneRedshiftManageAccessRolePolicyAmazon이 데이터에 대한 게시 및 액세스 권한을 DataZone 허용할 수 있는 권한을 부여하는 새 정책을 DataZone 추가했습니다. 자세한 내용은 AWS 관리형 정책에 대한 Amazon DataZone 업데이트를 참조하십시오.	2023년 9월 12일
AmazonDataZoneRedshiftGlueProvisioningPolicy - 새 정책	Amazon은 지원되는 데이터 소스와 상호 AmazonDataZoneRedshiftGlueProvisioningPolicy운용하는 데 필요한 권한을 DataZone Amazon에 부여하는 새 정책을 DataZone 추가했습니다. 자세한 내용은 AWS 관리형 정책에 대한 Amazon DataZone 업데이트를 참조하십시오.	2023년 9월 12일

AmazonDataZoneGlueManageAccessRolePolicy - 새 정책	Amazon은 AWS Glue 데이터를 카탈로그에 게시할 수 있는 DataZone 권한을 Amazon에 AmazonDataZoneGlueManageAccessRolePolicy부여한다는 새 정책을 DataZone 추가했습니다. 또한 Amazon에 카탈로그에 있는 AWS Glue 게시 자산에 대한 액세스 DataZone 권한을 부여하거나 액세스 권한을 취소할 수 있는 권한을 부여합니다. 자세한 내용은 AWS 관리형 정책에 대한 Amazon DataZone 업데이트를 참조하십시오.	2023년 9월 12일
AmazonDataZoneFullUserAccess - 새 정책	Amazon은 데이터 포털을 DataZone 통해 Amazon에 대한 전체 액세스 권한을 AmazonDataZoneFullUserAccess부여하는 새로운 정책을 DataZone 추가했습니다. 자세한 내용은 AWS 관리형 정책에 대한 Amazon DataZone 업데이트를 참조하십시오.	2023년 9월 12일
AmazonDataZoneFullAccess - 새 정책	Amazon은 AWS 관리 콘솔을 DataZone 통해 Amazon에 대한 전체 액세스를 AmazonDataZoneFullAccess제공하는 새로운 정책을 DataZone 추가했습니다. 자세한 내용은 AWS 관리형 정책에 대한 Amazon DataZone 업데이트를 참조하십시오.	2023년 9월 12일

AmazonDataZoneEnvironmentRolePermissionsBoundary - 새 정책	Amazon은 연결된 프로비저닝된 IAM 보안 주체를 제한하는 새 정책을 DataZone 추가했습니다. AmazonDataZoneEnvironmentRolePermissionsBoundary 자세한 내용은 AWS 관리형 정책에 대한 Amazon DataZone 업데이트를 참조하십시오.	2023년 9월 12일
관리형 정책 업데이트	AmazonDataZonePreviewConsoleFullAccess 관리형 정책 업데이트. 자세한 내용은 AWS 관리형 정책에 대한 Amazon DataZone 업데이트를 참조하십시오.	2023년 6월 13일
관리형 정책 업데이트	AmazonDataZoneProjectDeploymentPermissionsBoundary 관리형 정책 업데이트. 자세한 내용은 AWS 관리형 정책에 대한 Amazon DataZone 업데이트를 참조하십시오.	2023년 4월 3일
???	Amazon DataZone (프리뷰) 사용 설명서의 최초 릴리스.	2023년 3월 29일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.